

**NSA Office of the Inspector General Releases Three Reports**

**17 February 2016**

The National Security Agency (NSA) is releasing today three reports by NSA's Inspector General about the Agency's compliance with a current and former statute authorizing electronic surveillance. The reports detail steps NSA has taken to adhere to the law and highlight the importance of these legal authorities to the Agency's national security mission. They also reveal some procedural and other deficiencies that have been subsequently corrected. NSA reported the incidents to Congress as required. All three reports – more than 300 pages total – confirmed that there had been no cases of intentional violation of laws. NSA released the reports under a Freedom of Information Act request. They are being published on NSA.gov to help raise public awareness of the Agency's foreign intelligence mission and to highlight the Agency's ongoing commitment to compliance with the law. The NSA Inspector General's rigorous, independent, and continuous reviews are an essential part of the Agency's extensive oversight.

These reports, issued over a five-year period beginning in 2010, concern NSA activities conducted pursuant to two authorities: Section 702 of the Foreign Intelligence Surveillance Act (FISA), which authorizes targeted surveillance of foreign persons located outside the United States in certain cases, and Section 215 of the USA PATRIOT Act, which was replaced last year by the USA FREEDOM Act. NSA itself initiated two of the reports, and one was requested by members of the Senate Judiciary Committee. Below are highlights from these NSA Office of the Inspector General (OIG) reports.

**NSA OIG report ST-14-0002.** This report, issued on February 20, 2015, was compiled by the OIG at the request of members of the Senate Judiciary Committee. The OIG reviewed the controls implemented by NSA in carrying out activities pursuant to two FISA authorities. The first was Section 702, which was enacted as part of the FISA Amendments Act of 2008 and authorizes the targeting of non-U.S. persons reasonably believed to be outside the United States to acquire critical foreign intelligence information. This collection authority is one of the Intelligence Community's most significant tools for the detection, identification, and disruption of terrorist threats to the United States and its allies. The second authority examined by the OIG was Section 215 of the USA PATRIOT Act. Pursuant to Section 215, NSA was authorized to collect in bulk certain telephone metadata. This program operated from 2006 until its termination by statute on November 28, 2015. Section 215 was amended by the USA FREEDOM Act, which was enacted on June 2, 2015, and became effective on November 29, 2015. The USA FREEDOM Act made significant changes to NSA's authority to collect telephone metadata pursuant to the Foreign Intelligence Surveillance Act and was not the subject of OIG's review, so significant portions of the report are no longer relevant to NSA's activities.

The report presents a detailed, comprehensive picture of the operation of the Section 702 program. Specifically, it describes the extensive internal and external oversight and compliance reg-

including access restrictions, training requirements, and technical controls – as well as limits on data retention and dissemination of information. The report also notes a number of unintentional compliance failures and describes the controls put in place to mitigate recurrence. The report further notes that Section 702 contributes significantly to NSA's mission.

**NSA OIG report, ST-11-0009.** This report focused solely on Section 702 and was issued on March 29, 2013. It reviewed the system of management controls that NSA implemented, including training, access, and multiple levels of review and oversight. The OIG did not identify any areas of non-compliance. It recommended several areas in which controls over compliance with Section 702 could be improved, including a lack of clear guidance to analysts, inadequate documentation, and insufficient training in some instances. In each case, NSA's Signals Intelligence Directorate agreed with the OIG recommendations and implemented corrective action plans.

**NSA OIG report AU-10-0023.** This report, which covered only certain aspects of NSA's implementation of Section 702, was issued on November 24, 2010. Specifically, the report reviewed the process by which NSA transitioned from collection pursuant to Section 702 to other authorities under FISA. The OIG identified the lack of a standardized process, which created the potential for gaps in lawful surveillance coverage. The Agency has since implemented an improved transition process. Moreover, Section 701 of the USA FREEDOM Act subsequently clarified surveillance procedures in that regard.

The National Security Agency is tasked with a complex foreign intelligence mission and is dedicated in its respect for U.S. laws and policies. There is a robust internal and external oversight structure in which all three branches of government play a key role, as well as a rigorous internal compliance program. The three NSA OIG reports published *here* are intended to help raise public awareness of the Agency's mission and to highlight ongoing commitment to compliance with the law.

---

**NATIONAL SECURITY AGENCY/CENTRAL SECURITY  
SERVICE**



**(U) Final Report of the Audit on the FISA Amendments  
Act §702 Datasizing Requirements**

**AU-10-0023**

**24 November 2010**

DERIVED FROM: NSA/CSS Manual 1-52

DATED: 08 January 2007

DECLASSIFY ON: ~~20320108~~

~~TOP SECRET//COMINT//NOFORN~~**(U) NSA OFFICE OF THE INSPECTOR GENERAL**

(U) The NSA Office of the Inspector General (OIG) conducts audits, investigations, inspections, and special studies. Its mission is to ensure the integrity, efficiency, and effectiveness of NSA operations, provide intelligence oversight, protect against fraud, waste, and mismanagement of resources, and ensure that NSA activities are conducted in compliance with the law. The OIG also serves as an ombudsman, assisting Agency employees, civilian and military, with complaints and questions.

**(U) Intelligence Oversight**

(U) The OIG Office of Intelligence Oversight reviews NSA's most sensitive and high-risk programs for compliance with the law.

**(U) Audits**

(U) The OIG Office of Audits within the OIG provides independent assessments of programs and organizations. Performance audit evaluate the effectiveness and efficiency of entities and programs and assess whether NSA operations comply with federal policies. Information Technology audits determine whether IT solutions meet customer requirements, while conforming to information assurance standards. All audits are conducted in accordance with standards established by the Comptroller General of the United States.

**(U) Investigations and Special Inquiries**

(U) The OIG Office of Investigations administers a system for receiving and tracking requests for assistance and complaints about fraud, waste, and mismanagement. Investigations and special inquiries may be undertaken as a result of such requests and complaints (including anonymous tips); the request of management; as the result of questions that surface during inspections and audits; or at the initiative of the Inspector General.

**(U) Field Inspections**

(U) The Office of Field Inspections conducts site reviews as part of the OIG's annual plan or by management request. Inspections yield accurate, up-to-date information on the effectiveness and efficiency of field operations and support programs, along with an assessment of compliance with federal policy. The Office partners with Inspectors General of Service Cryptologic Components and the Intelligence Community Agencies to conduct joint inspections of consolidated cryptologic facilities.

[REDACTED]



**OFFICE OF THE INSPECTOR GENERAL  
NATIONAL SECURITY AGENCY  
CENTRAL SECURITY SERVICE**

24 November 2010  
IG-112266-10

**TO: DISTRIBUTION**

**SUBJECT: (U) Audit of the FISA Amendments Act (FAA) §702 Detasking Requirements (AU-10-0023)— ACTION MEMORANDUM**

1. (U) This report summarizes the results of our audit of the FISA Amendments Act (FAA) §702 Detasking Requirements (AU-10-0023) and incorporates management's response to the draft report.

2. (U//FOUO) As required by NSA/CSSS Policy 1-60, NSA/CSSS *Office of the Inspector General*, actions on OIG audit recommendations are subject to monitoring and follow-up until completion. Therefore, we ask that you provide a written status report concerning each planned corrective action categorized as "OPEN." If you propose that a recommendation be considered closed, please provide sufficient information to show that actions have been taken to correct the deficiency. If a planned action will not be completed by the original target completion date, please state the reason for the delay and provide a revised target completion date. Status reports should be sent to [REDACTED] Assistant Inspector General for Follow-up, at OPS 2B, Suite 6247, within 15 calendar days after each target completion date.

3. (U//FOUO) We appreciate the courtesy and cooperation extended to the auditors throughout the review. For additional information, please contact [REDACTED] on 963-0957 or via e-mail at [REDACTED]

(b) (3) -P.L. 86-36

  
George Ellard  
Inspector General

DISTRIBUTION:

COS  
OGC  
SID

CC:

SID [REDACTED]  
SID [REDACTED]  
SID [REDACTED] (b) (3) P.L. 86-36  
SID [REDACTED]  
SAE [REDACTED]  
S2I [REDACTED]  
SV4 [REDACTED]  
IG [REDACTED]  
D11 [REDACTED]  
D11 [REDACTED] J  
D12  
D14

**(U) TABLE OF CONTENTS**

|   |            |
|---|------------|
| <b>(U) EXECUTIVE SUMMARY.....</b>                           | <b>iii</b> |
| <b>I. (U) INTRODUCTION.....</b>                             | <b>1</b>   |
| <b>II. (U) FINDING AND RECOMMENDATION.....</b>              | <b>5</b>   |
| <b>(U) FINDING: Gaps in [REDACTED] Coverage Exist .....</b> | <b>55</b>  |
| <b>(U) ACRONYMS AND ORGANIZATIONS.....</b>                  | <b>19</b>  |
| <br><b>(b)(3) HPL.866-36</b>                                |            |
| <b>(U) APPENDIX A: About the Audit</b>                      |            |
| <b>(U) APPENDIX B: Data Analysis</b>                        |            |
| <b>(U) APPENDIX C: Full Text of Management Responses</b>    |            |

(U) This page intentionally left blank.

**(U) EXECUTIVE SUMMARY**

(b) (1)  
(b) (3)-P.L. 86-36  
(b) (3)-50 USC 3024 (i)

**(U) OVERVIEW**

(S//SI//REL TO USA, FVEY) Section 702 of the Foreign Intelligence Surveillance Act (FISA) Amendments Act of 2008 (FAA), has strengthened Signals Intelligence (SIGINT) collection, particularly against terrorist targets. From September 2008 to March 2010, the number of SIGINT reports that incorporated FAA §702 sourced collection [redacted]

(TS//SI//NF) Under the law, collection under FAA §702 must cease in certain circumstances, potentially resulting in a gap in coverage. To regain coverage, NSA must transition to another authority for continued collection, such as a FBI FISA Order. The Agency does not have a consistent process to ensure a seamless transition from FAA §702 authority to FBI FISA Orders.

**(U) HIGHLIGHTS**

(U) Gaps. In [redacted] coverage exist

(TS//SI//REL TO USA, FVEY) Analysis of detasking for FAA §702 compliance

(b)(3)-P.L. 86-36  
(U) Significance of [redacted]

(TS//SI//NF)

(b) (1)

(b) (3)-P.L. 86-36  
(b) (3)-50 USC 3024 (i)

(S//SI//REL TO USA, FVEY) Need for standardized process

(TS//SI//NF) The Agency lacks a standardized process

(U//FOUO) Management Response

(U//FOUO) The recommendation is being addressed by management.

(b) (1)  
(b) (3)-P.L. 86-36  
(b) (3)-50 USC 3024 (i)

-TOP SECRET//COMINT//NOFORN

(U) This page intentionally left blank.

## I. (U) INTRODUCTION

### (U) Background

~~(TS//SI//NF)~~ Section 702 of the Foreign Intelligence Surveillance Act (FISA) Amendments Act of 2008 (FAA), enhances surveillance against foreign nationals outside the United States.

1 ~~(TS//SI//NF)~~ §702 effectively broadened access to critical targets of interest, particularly terrorists. From September 2008, when FAA was implemented, to March 2010, the number of Signals Intelligence (SIGINT) reports that incorporated §702 sourced collection [REDACTED]

(b) (1)

(b) (3) -P.L. 86-36

~~(TS//SI//NF)~~ Collection under FAA §702 must cease under certain circumstances. Detasking is required when a target is determined to be entering or to have entered the United States.

Collection also must cease when a target is found to be a U.S.

[REDACTED] To regain coverage of such a target, collection must transition to another authority, for example, a Federal Bureau of Investigation (FBI) FISA Order. The transition from FAA §702 to another authority may not be seamless, thereby creating a gap in coverage and potentially causing a risk to U.S. security. This audit assessed the circumstances and extent of the FAA §702 coverage gap by examining tasking and detasking records, FBI FISA data, traffic collected and punged, and SIGINT reporting.

### (U) FAA §702

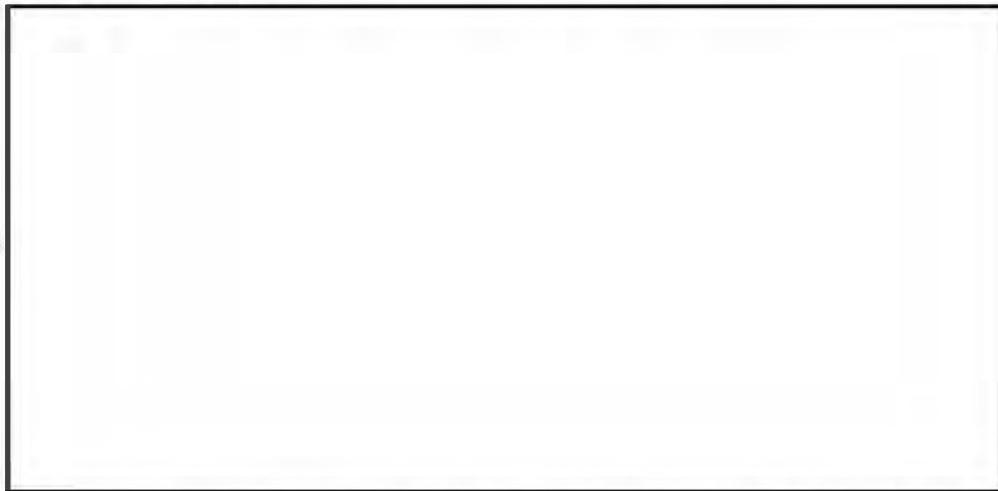
~~(TS//SI//NF)~~ FAA §702 allows NSA to use the assistance of U.S. telecommunications and Internet service providers to target non-USPs outside the United States. After the Attorney General and the Director of National Intelligence issue a joint certification that certain statutory requirements have been met and the certification is approved by the FISC, NSA may conduct foreign intelligence surveillance of the content of communications. The certification includes an affirmation that the surveillance targets only non-USPs reasonably believed to be outside the United States. The certification is submitted to the FISC and typically is approved for one year. Acquisition under a certification must adhere to targeting and minimization procedures approved by the Court. As of August

2010, NSA was authorized to conduct FAA §702 collection under [redacted] certifications.

(B)(1)

(b) (3) -P.L. 86-36

(b) (3)-500 USC 3024(i)



(U//FOUO) Other, FISA authorities provide alternative means to obtain collection against foreign intelligence targets when NSA must stop collection (detask) pursuant to FAA §702.

- (U) **FAA §704**

(U//FOUO) *Other Acquisitions Targeting USPs Outside the United States.* A FISC Order is required, but surveillance techniques are not reviewed by the court.

- (U) **FAA §705b**

(U//FOUO) *Joint Applications and Concurrent Applications.* When a FISA Order that authorizes surveillance of a target inside the United States is in place, the Attorney General can authorize targeting while the USP is reasonably believed to be outside the United States.

- (U) **FBI FISA Order**

(S//SI//REL TO FVEY) The FBI is authorized under a FISC Order to perform searchless and electronic surveillance against agents of a foreign power. Under FISC ticket number [redacted] (known as the Raw Take Sharing Order) dated July 2002, NSA is able to receive most FBI FISA collection.

(b) (1)

(b) (3) -P.L. 86-36

(b) (3)-500 USC 3024(i)

**(U) Increased use of FAA §702 Authority**

(S//SI//REL TO USA, FVEY) According to analysts in the Signals Intelligence Directorate (SID), collection under FAA §702 authority is productive and grew in the 19 months between September 2008 and March 2010. Increased tasking under FAA §702 authority has resulted in increased SIGINT reporting. The Agency has also experienced an increase in compliance-related detaskings of selectors.

- (U) **Tasking**  
~~(S//SI//REL TO USA, FVEY)~~ Tasking by selected [REDACTED]  
increased [REDACTED]
- (U) **Detasking** TO usA, FVEYI compliance -relatedt detasking 1  
~~(S//SI//REL TO USA, FVEY)~~ Compliance-related detasking significantly increased [REDACTED]
- (U) **SIGINT reporting**  
~~(S//SI//REL TO USA, FVEY)~~ Reporti based on collection under FAA §702 authority increased [REDACTED]

~~(S//SI//REL TO USA, FWMY)~~

**(U) NSA oversight of FAA §702 collection**

~~(S//SI//REL TO USA, FVEY)~~ In addition to the analysts' obligation to review the status of their selectors, the SID Oversight and Compliance Office (SV) is responsible for monitoring compliance with FAA §702 and tracking detasking. SV monitors selectors through special tools to ensure compliance. [REDACTED] (b) (3)-PLL. 86-36

[REDACTED] When a Compliance problem exists, SV contacts the Targetingg Office of Primary Interest (TOPI) and requests that its personnel research the selector before detasking. SV is also responsible for maintaining a Protect America Act (PAA)/FAA Incident database to record and track incidents and provide that information for external oversight by the Department of Justice (DoJ) and the Office of the Director of National Intelligence.

(U) This page intentionally left blank.

## II. (U) FINDING AND RECOMMENDATION

(U) FINDING: Gaps in [REDACTED] coverage Exist.

(b) (3) - P.L. 86-36

(TS//SI//NF) Although FAA §702 has provided important SIGINT collection, the Agency has experienced [REDACTED] coverage gaps when transitioning from FAA §702 to another authority. [REDACTED]

[REDACTED]

(U) FAA §702 Implementation

### (U) FAA §702 procedures

(TS//SI//NF) FAA §702 requires that NSA adopt procedures to ensure that its collection targets are non-USPs reasonably believed to be outside the United States and to ensure that the Agency does not intentionally acquire communications known to be purely domestic. NSA must also establish minimization procedures that reasonably balance its foreign intelligence needs against the privacy interests of USPs with respect to the collection, retention, and dissemination of information.

### (U) FAA §702 detaskings for compliance

(U//FOUO) In certain circumstances, NSA must detask selectors to maintain compliance with FAA §702 and approved targeting and minimization procedures. There are three broad reasons for detasking.

- (U) Roamers

(S//SI//REL TO USA, FVEY) The foreign target is initially believed to be overseas, but it is subsequently determined that the target has entered the United States. [REDACTED]

(b) (1)

(b) (3) - P.L. 86-36

- (U//FOUO) USP status determined after tasking

(S//SI//REL TO USA, FVEY) The target is overseas and believed to be foreign, but NSA subsequently determines that the target is a USP overseas.

(b) (1)

(b) (3) - P.L. 86-36

(b) (3) - 50 USC 3024 (i)

(S//SI//REL TO USA, FVEY)

(b) (1)  
(b) (3) -P.L. 86-36

[REDACTED]

NSA must detask the account from FAA §702 collection.

~~(TS//SI//NF)~~ Once NSA determines that a target is a USP, is roaming in the United States, or [REDACTED]  
 D [REDACTED] NSA must detask associated selectors from collection under FAA §702 authority and purge related SIGINT holdings from all databases. To avoid a break in coverage, other authorities must be sought if the target remains of interest and is an agent of a foreign power (e.g., §704, §705b, and/or FBI FISA).

**(C) Compliance detaskings few in context, but potential risk is great**

~~(SI//SI//REL TO USA,~~

~~INFO)~~ The number of selectors that are detasked for compliance reasons from collection under FAA §702 authority is small compared with all SIGINT selector tasking as of March 2010 [REDACTED]

however, loss of FAA §702 collection on potentially high-interest selectors, particularly those related to [REDACTED] poses a risk when transition to alternative coverage is not seamless.

**(U//FOUO)** FAA 702 detasked Selectors compared to all FAA tasking and total SIGINT Selectors

(b) (1)  
(b) (3)

-P.L. 86-36

(b) (1)

(b) (3) -P.L. 86-36

**(U) Defining the FAA §702 gap in coverage**

~~(TS//SI//NF)~~ The gap in coverage is the collection lost in the time between detasking selectors from FAA §702 collection authority and initiation of collection under another authority (e.g., §704, §705b, or FBI FISA). For non-FAA §702 coverage, a higher legal standard, individualized probable cause, is required to secure a FISA order. In some cases, the Government may not be able to assemble facts sufficient to satisfy the probable cause standard: [REDACTED]

(U) Audit Focus 9A [redacted]

(U) Audit universe of FAA §702 detaskings

(S//SI//REL TO USA, FVEY) To determine the extent of the coverage gaps, we identified every Digital Network Intelligence (DNI) and Dialed Number Recognition (DNR) selector that was tasked to comply with FAA §702 after enactment of the FAA in July 2008. By examining [redacted] tasking records and SV's PAA/FAA Incidents database, we identified D [redacted] relevant tasked DNI and DNR selectors. These selectors were drawn from [redacted] FAA §702 certifications [redacted]

(b) (3)-P.L. 86-36

(b) (1)  
(b) (3)-P.L. 86-36

(b) (3)-50 USC 3024(i)

(U) Focus: contribution of collection under FAA §702 authority to [redacted] reporting

(S//SI//REL TO USA, FVEY) From September 2008 to March 2010, FAA §702 collection contributed to an increasing percentage of [redacted] reporting. Overall, the increase was from [redacted] percent to [redacted] percent.

(S//SI//REL TO USA, FVEY)

Percentage of [redacted] Reporters with Contributions from FAA  
(September 2008 - March 2010)

(S//SI//REL TO USA, FVEY)

(b) (3) PPL. 86-36

(U//FOUO) Audit sample focuses on [ ] DNI selectors

(S//SI//REL TO USA, FVEY) From the universe of [ ] tasked DNI and DNR selectors, we identified [ ] DNI selectors for detailed selector-by-selector gap analysis (see Appendix B for scope and methodology). DNI selectors represented the large majority of FAA §702 detaskings in the sample (93 percent). In addition, [ ] selectors accounted for [ ] percent of tasked FAA

(b) (1)  
(b) (3) -P. L. 86-36

(U//FOUO) Audit sample focuses on [ ] DNI selectors as indicated in the adjacent diagram. The large quantity of taskings and detaskings coupled with the significant role of FAA §702 on [ ] reporting, as well as the high risk that a gap in [ ] coverage poses, prompted our focus on [ ] DNI detaskings.

#### (U) Effective Collection Priority

(S//SI//REL TO

(b) (1)  
(b) (3) -P. L. 86-36

(U//SI//REL TO USA, FVEY) To understand better the priority of tasking and forwarding of collection for these [ ] selectors, we obtained the Effective Collection Priority (ECP) of the [ ] selectors under review. ECP is derived from two values: national SIGINT priority and collection precedence [ ]

[ ] ECP values range from one through nine, with one being the highest priority. For the [ ] selectors that we identified, the average ECP was 2.52, indicating that these selectors are of high priority.

#### (U) Effect of Gaps on SIGINT Collection and Reporting

(TS//SI//NF) To determine the effects of FAA §702 detasking on [ ] SIGINT collection and reporting, we analyzed the [ ] selectors during a 13-month period (February 2009 to March 2010). [ ]

(b) (1)  
(b) (3) -P. L. 86-36

(b) (1)

(b) (3)-P.L. 86-36

(U) DCollection Coverage Gap Analysis

(TS//SI//NF)

(TS//SI//NF)

(b) (1)

(b) (3)-P.L. 86-36

(U//FOUO) Time delay poses risk on productive selectors

(TS//SI//NF)

(b) (1)

(b) (3) -P. L. 86-36

(U) Minimal delay between highest interest selectors

(TS//SI//NF)

(b) (1)

(b) (3) -P. L. 86-36

(b) (3) -50 USC 3024(i)

r ~ 1

could

(U) Majority of ns selectors dropped from collection

(b) (3) -P. L. 86-36

(TS//SI//NF)

(b) (1)

(b) (3) -P. L. 86-36

(b) (3) -50 USC 3024(i)

## (U) Selections not Retasked

(TS//SI//NF)

| Reason Selector Was not Retasked | No. of Detaskings | Percentage of Total |
|----------------------------------|-------------------|---------------------|
|                                  |                   |                     |
| Total                            |                   | 100.00%             |

(TS//SI//NF)

## (U) Lack of Systematic Process

(b)(1)  
(b)(3)-P.L. 86-36

(U) [REDACTED] (b)(3)-P.L. 86-36  
 (TS//SI//NF) [REDACTED] Production Center has faced challenges in achieving seamless coverage off targets while maintaining compliance with FAA §702 requirements; [REDACTED]

(b)(1)  
(b)(3)-P.L. 86-36  
(b)(3)-50 USC 3024(i)

(b)(3)-P.L. 8

(U//FOUO) [REDACTED]  
 (TS//SI//NF) [REDACTED]

## (U) Need for consistent process

(TS//SI//NF)

^ (U//FOUO) [REDACTED]

(b)(3)-P.L. 8

(b)(1)  
(b)(3)-P.L.86-36  
(b)(3)-50 USC 3024(i)

(b)(3)-P.L.88

| (TS//SI//NF) |                  |            |
|--------------|------------------|------------|
| Gap          | No. of Selectors | Percentage |
|              |                  | Total 100% |

(b)(3)-P.L. 86-36

(TS//SI//NF)

(b)(1)  
(b)(3)-P.L. 86-36

(U//FOUO)  
(TS//SI//NF)

1. (TS//SI//NF) After the Agency detasks an FAA §702 selector,

(b)(3)-P.L. 86-36  
(b)(3)-18 USC 798  
(b)(3)-50 USC 3024(i)

2. (TS//SI//NF) TOPIs can directly notify [REDACTED]

(b)(1)  
(b)(3)-P.L. 86-36

3. (TS//SI//NF) After normal duty hours, NSA's

4. (TS//SI//NF) Agency analysts can send [REDACTED]

(TS//SI//NF)

(TS//SI//NF) In addition, in September 2009, at the request of the NSA Director, an Emergency Authorization Concept of Operations was developed [REDACTED] and the Office of General Counsel (OGC) to outline a detailed process for maintaining coverage [REDACTED]

<sup>3</sup> (S//SI//REL TO USA, FWD EX)

TOP SECRET//COMINT//NOFORN (b)(1)

(U//FOUO) Lack of understanding of the handoff process

(TS//SI//NF)

{b}(1)  
(b)(3)-P.L.866366  
(b)(3)-50 USC 3024(i)

(U//FOUO)

### Case studies

(TS//SI//NF)

(b)(1)  
(b)(3)-P.L.866366  
(b)(3)-50 USC 3024(i)

1. (TS//SI//REL TO USA, FVEW) Informal, but nearly seamless:

(TS//SI//REL TO USA, FVEW)

(b)(1)  
(b)(3)-P.L.866366  
(b)(3)-18 USC 79  
(b)(3)-50 USC 30

(TS//SI//NF)

(b)(1)  
(b)(3)-P.L.866366  
(b)(3)-50 USC 3024(i)

(TS//SI//NF) Selectors Associated with [REDACTED]

(b)(1)  
(b)(3)-P.L.8

(TS//SI//NF)

### Selectors

{6>HT  
(b)(1)  
(b)(3)-P.L.866366

(TS//SI//NF)

(TS//SI//NF) NSA, the Central Intelligence Agency, and the FBI

(b)(1)  
(b)(3)-P.L. 86-36

2. (TS//SI//REL TO USA, FVEY)

(TS//SI//NF)

(b)(ff)  
(b)(3)-P.L. 86-36  
(b)(3)-50 USC 3024(i)

(TS//SI//NF) Selectors Associated with [REDACTED]

(TS//SI//NF)

(b)(1)  
(b)(3)-P.L. 86-36

(TS//SI//NF)

(TS//SI//REL TO USA, FVEY) These selectors had been placed under FAA §702 coverage [REDACTED]

(b)(1)

(b)(3)-P.L. 8

[REDACTED] because they were used by several persons associated with [REDACTED]

(b)(1)  
(b)(3)-P.L. 86-36  
(b)(3)-50 USC 3024(i)

(TS//SI//NF) [REDACTED] analysts initially did not know who to contact about obtaining alternative coverage and were not clear about what could be obtained from FAA §705b tasking and how this tasking [REDACTED] Ultimately, the analysts [REDACTED]

(b)(1)

(b)(3)-P.L. 8

4. (S//SI//REL TO USA, FVEY)

(b)(3)-P.L. 8

were provided guidance internally [redacted]

(b)(1)  
(b)(3)-P.L. 86-36  
(b)(3)-50 USC 3024(i)

(TS//SI//NF)

occur because not all analysts in the office are familiar with these new procedures.

3. (TS//SI//REL TO USA, FVEY) Limited feedback and a long delay:

(TS//SI//NF)

(b)(1)  
(b)(3)-P.L. 8

(b)(1)  
(b)(3)-P.L. 86-36  
(b)(3)-50 USC 3024(i)

(TS//SI//NF) Selector Associated with [redacted]

(TS//SI//NF)

(TS//SI//NF)

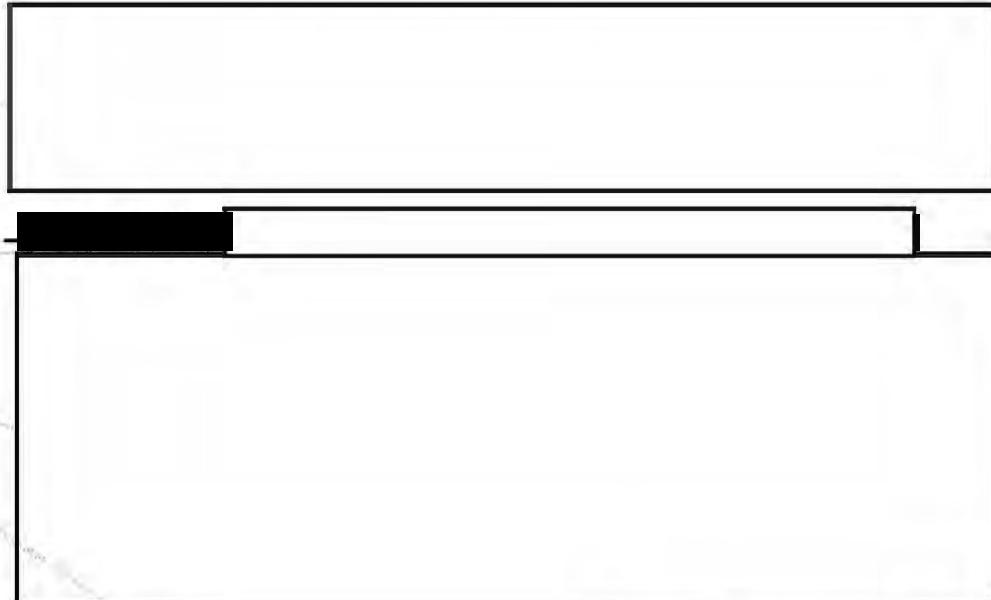
(TS//SI//NF) Shortly after tasking on the selector had been initiated.]

(b)(1)  
(b)(3)-P.L. 86-36  
(b)(3)-50 USC 3024(i)

<sup>5</sup> (S//SI//REL TO USA, FVEY) SV uses [redacted] to monitor tasked selectors to ensure foreignness and compliance with the law.

-TOP SECRET//COMINT//NOFORN•{

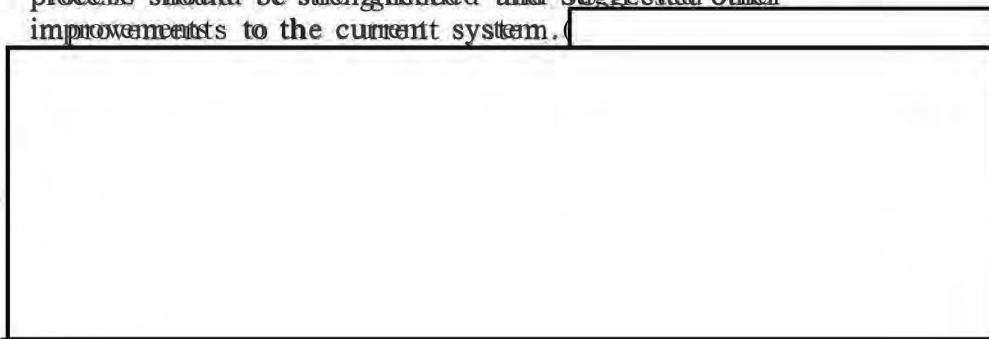
(b)(1)  
(b)(3)-P.L. 86-36  
(b)(3)-50 USC 3024(i)



(U) [redacted] suggest improvements

(b)(3)-P.L. 86-36

(TS//SI//NF) [redacted] agreed that a standardized process would improve the timeliness [redacted]. They also concluded that the process should be strengthened and suggested other improvements to the current system. [redacted]



### Recommendation

(TS//SI//NF) Establish a standardized process for [redacted] when it is determined that coverage should continue after selectors are detached from FAA §702 collection.

(ACTION: SID with OGC)

(b)(1)  
(b)(3)-P.L. 86-36  
(b)(3)-50 USC 3024(i)

### (U) Management Response

CONCUR. (U//FOUO) [redacted] and OGC concur with OIG's recommendation. Corrective action is under way and will be completed as soon as possible, [redacted] (b)(3)-P.L. 86-36

~~TOP SECRET//COMINT//NOFORN~~

Successful completion within this timeframe is contingent upon direct involvement from SV and S1 as they are owners of mission components that are directly tied to the transition process (see Appendix C for full text of management comments).

**(U) OIG Comment**

(U) Planned actions meet the intent of the recommendation.

**(U) Loss of Collection**

(b)(3)-P.L. 86-36

(S//SI//REL TO USA, FVEY) We also grouped the  selectors reviewed by the reason for detasking.

(TS//SI//NF)

**Circumstances of Detasking**

(b)(1)  
(b)(3)-P.L. 86-36  
(b)(3)-50 USC 3024(i)

(TS//SI//NF)

(TS//SI//NF)

**(U) Significance of**

(b)(3)-P.L. 86-36

(TS//SI//NF)

(U//FOUO) Strict guidance on detasking [REDACTED] (b)(3)-P.L. 86-36  
(S//SI//REL TO USA, FVEY) Strict guidance from DoJ and OGC

(TS//SI//NF) [REDACTED]

(b)(1)  
(b)(3)-P.L. 86-36  
(b)(3)-50 USC 3024(i)

(U) Action taken

(TS//SI//NF) [REDACTED] the DIRNSA, along with the (b)(3)-P.L. 86-36 Attorney General and the acting Director of National Intelligence, filed with the FISC FAA §702 certification/renewal documents related to targeting and minimization procedures for the [REDACTED]

(TS//SI//NF) [REDACTED] NSA learned that the FISC was concerned with the proposed changes to the minimization procedures. DoJ and NSA are exploring alternatives to address the matter while continuing to operate under the existing procedures.

## (U) ACRONYMS AND ORGANIZATIONS

|                      |   |
|----------------------|---|
| [REDACTED]           | (U) [REDACTED]  |
| CIA                  | (U) Central Intelligence Agency   |
| [REDACTED] (U//FOUO) | (U) [REDACTED]  |
| DIRNSA               | (U) Director, NSA   |
| DNI                  | (U) [REDACTED] Digital Network Intelligence (b)(3)-P.L. 86-36                               |
| DNR                  | (U) Dialed Number Recognition   |
| DoJ                  | (U) Department of Justice   |
| ECP                  | (U) Effective Collection Priority   |
| FAA                  | (U) Foreign Intelligence Surveillance Act of 1978 (FISA) Amendments Act of 2008             |
| FBI                  | (U) Federal Bureau of Investigation   |
| FISA                 | (U) Foreign Intelligence Surveillance Act of 1978   |
| FISC                 | (U) Foreign Intelligence Surveillance Court   |
| [REDACTED]           | (U) [REDACTED]  |
| OGC                  | (U) Office of General Counsel   |
| PAA                  | (U) Protect America Act   |
| SID                  | (U) Signals Intelligence Directorate  |
| SIGINT               | (U) Signals Intelligence  |
| SV                   | (U) [REDACTED] Signals Intelligence Directorate, Oversight and Compliance                   |
| SV4                  | (U) [REDACTED] Signals Intelligence Directorate, Oversight and Compliance, FISA Authorities |
| TOPI                 | (U) [REDACTED] Targeting Office of Primary Interest   |
| USP                  | (U) United States Person  |

(U) This page intentionally left blank.

**(U) APPENDIX A****(U) About the Audit**

(U) This page intentionally left blank.

## (U) ABOUT THE AUDIT

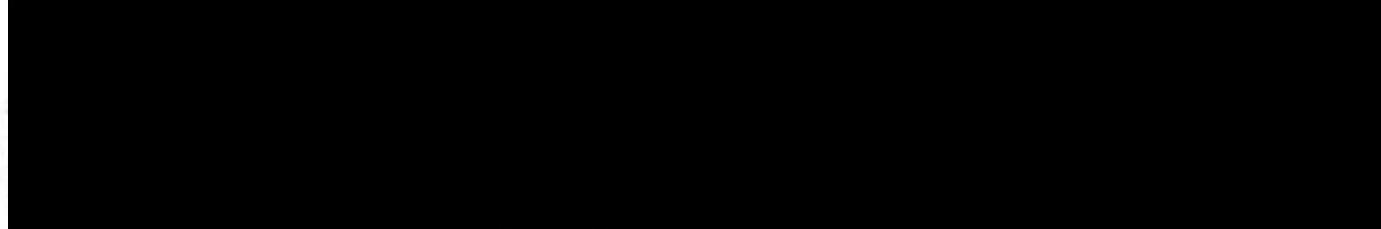
### (U) Objectives

(U) The audit objective was to document the circumstances and the extent of dropped Signals Intelligence(SIGINT) collection as a result of Foreign Intelligence Surveillance Act of 1978 (FISA) Amendments Act of 2008 (FAA) §702 restrictions.

### (U) Scope and Methodology

(U) Conducted from February to August 2010, the audit examined the gaps in coverage when a selector is required to be detasked for compliance with FAA §702 and the measured effect of the lost coverage.

(U//FOUO) We reviewed current policies and laws pertaining to FAA §702. We obtained access to the Protect America Act (PAA)/FAA Incident database and reviewed reported incidents from 10 July 2008 (when the FAA became law) through 4 March 2010 and documented actual instances when SIGINT collection was stopped to comply with §702. See Appendix C - Data Analysis for our data sources.



### (U) SID Oversight and Compliance

(U//FOUO) To gain an understanding of the Agency's process for documenting and reporting incidents and violations, we met with the SV staff. We obtained for our analysis information from SV's PAA/FAA Incidents database on selectors that were detasked because of FAA §702 restrictions.

### (U) Office of General Counsel

(U//FOUO) We met with the OGC FAA liaison to gain the overall legal perspective of the implementation of FAA §702. We also met with the Acting General Counsel to discuss the nature of collection restrictions that are inherent in NSA's legal authorities. In addition, we discussed whether the current law is sufficient for NSA to achieve its mission goals.

(U) [REDACTED]

(U//FOUO) We met with technical leadership in the [REDACTED] to gain an understanding of the legal, policy, and compliance constraints in the [REDACTED]

(b)(3)-P.L. 86-36

[REDACTED] analytic environment, specifically related to FAA §702. Case studies regarding [REDACTED] selectors that were declassified because of FAA §702 restrictions were conducted; [REDACTED]

[REDACTED] when a selector was declassified was discussed with [REDACTED] analysts. We obtained the analysts' opinions about the effect of collection on their work, including specific benefits and obstacles of the FAA §702 authority.

#### **(U) FAA implementation leads**

(U//FOUO) We met with the Analysis & Production FAA leads who are charged with overseeing working groups, which are addressing problems with carrying out work under the FAA. They outline efforts on analytic training and coordinate with the Department of Justice, OGC, and SV.

(S//SI//REL TO USA, FVEY)

(TS//SI//NF)

#### **(U) Tasking tool and data repository personnel**

(U//FOUO) We met with personnel in [REDACTED] to discuss the [REDACTED] and [REDACTED] tasking databases. We obtained extractions from these databases to assist in our review. In addition, we met with the [REDACTED] metrics team, [REDACTED] personnel, and a representative from SIGINT Strategy and Governance to gather additional data concerning tasking gaps, collection prioritization, and qualitative measures related to the FAA §702 selectors of interest.

(b)(3)-P.L. 86-36

L -3

(b)(1) P.L. 86-3  
(b)(3)-P.L. 86-36  
(b)(3)-50 USC 3024(i)  
(b)(3)-50 USC

#### **(U) Training**

(U//FOUO) We took the Legal Compliance and Minimization Procedures (USSID 18) training to obtain access to certain databases. In addition, we attended [REDACTED] training.

#### **(U) Government auditing standards**

(U) We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions according our audit objectives. We believe

that the evidence obtained provides a reasonable basis for our findings and conclusions according to our audit objectives.

#### **(U) Prior Coverage**

---

(U) The Office of the Inspector General has not performed any previous audits or inspections on FAA §702.

#### **(U) Use of Computer-Processed Data**

---

(U) To perform this audit, we used data that originated from the [redacted] the SV4 PAA/FAA "Recipients," [redacted] [redacted] (b)(3)-P.L.86-366 databases. We used the data to conduct a gap analysis on selectors that were deselected for FAA §702 compliance reasons. We did not determine the validity of these databases; however, we validated the data across multiple sources to ensure an accurate depiction of the data as used for our analysis.

#### **(U) Management Control Program**

---

(U) (FOUO) As part of the audit, we assessed the organization's control environment pertaining to the audit objectives, as set forth in NSA/CSSS Policy 7-3, *Internal Control Program*, 14 April 2006. We found that SV4's 2010 statement of assurance reported that a lack of upgrades of Information Technology systems and software application and lack of training and staffing could impede the SV4 mission.

~~TOP SECRET//COMINT//NOFORN~~

**(U) APPENDIX B**

**(U) Data Analysis**

(U) This page intentionally left blank.

**(U) DATA ANALYSIS****(U) Identification of Detasked Selectors**

(b)(3)-P.L. 86-36

(U//FOUO) We used the SV PAA/FAA incidents database and the [redacted] as sources of selectors that were detasked to maintain compliance with FAA §702.

(U//FOUO)

**SV4 PAA/FAA Incidents database**

(U//FOUO) We examined the SV4 PAA/FAA Incidents database, which contains a record of reportable incidents under the PAA/FAA. A reportable incident under PAA/FAA is one of the following:

(U//FOUO) The conduct of any SIGINT activity (collection, processing, retention or dissemination) using PAA collectors in a way that contravenes the terms of the PAA or the terms of the specific certification under which you are operating.<sup>6</sup> This includes any activity that runs counter to the Director's affidavit or the associated exhibits that describe the process for determining foreignness, the minimization procedures, or the targets authorized for collection under the certification.

(U//FOUO) The conduct of any SIGINT activity using PAA collectors without having a certification in place to cover the target being collected.

(b)(1)

(b)(3)-P.L. 86-36

(S//SI//REL TO USA, FVEY) We reviewed the records in the SV PAA/FAA Incidents database from 10 July 2008 (the inception of FAA) to 4 March 2010 and determined that there were a total of [redacted] incidents.

(U//FOUO) The records in the database are categorized by incident type. This allowed us to determine those that met the criteria for our review of detaskings related to compliance. The relevant incident types for further review are:

(b)(1)  
(b)(3)-P.L. 86-36  
(b)(3)-50 USC 3024(i)

- (S//SI//REL TO USA, FVEY) Roamers into the US
- (S//SI//REL TO USA, FVEY) [redacted]
- (S//SI//REL TO USA, FVEY) [redacted]
- (S//SI//REL TO USA, FVEY) Targets identified as a USP after tasking under §702

(U//FOUO) Incident types such as "analyst error" and "tasking error" did not relate to detasking to maintain compliance with §702; therefore, we eliminated these types of records from our review.

<sup>6</sup> (U) PAA was the predecessor to FAA.

(b)(3)-P.L. 86-36

(U//~~FOUO~~) [REDACTED]

(S//SI//REL TO USA, FVEW) [REDACTED] is the targeting tool used to submit and manage Digital Network Intelligence (DNI) targeting requests. To ensure that we obtained records of all detaskings related to §702 compliance, we requested from [REDACTED] tasking records a record of detaskings for any of the three following reasons<sup>7</sup>:

1. User is a USP
2. User is entering the United States
3. User is in the United States

(b)(3)-P.L. 86-36

(S//SI//REL TO USA, FVEW) The main purpose for requesting detasking records from [REDACTED] was to search for selectors that were detasked citing a reason "user is entering the United States" and that were not captured as incidents in the SV PAA/FAA Incidents database because they were detasked before the user actually roamed into the United States.

#### (U) Audit universe

(U//~~FOUO~~) We compared the results of the query with the selectors identified in the review of the PAA/FAA Incidents database and identified additional selectors that were detasked for compliance purposes.

(b)(1)  
(b)(3)-P.L. 86-36

(S//SI//REL TO USA, FVEW) From our review of the SV PAA/FAA Incidents and [REDACTED] detasking records, we identified a total universe of [REDACTED] unique selectors that were detasked for compliance reasons. The detaskings covered the [REDACTED] FAA §702 certifications:

(b)(3)-P.L. 86-36

[REDACTED] We were able to identify both detasked DNI and Dialed Number Recognition (DNR) selectors from the SV PAA/FAA Incidents database and detasked DNI selectors from [REDACTED] detasking records. The breakout of the selectors are detailed in the following table:

(b)(1)  
(b)(3)-P.L. 86-36  
(b)(3)-50 USC 3024(i)

<sup>7</sup> (U//~~FOUO~~) [REDACTED] did not formally include a "detask reason" field until an upgrade was performed in February 2009; therefore, our search within [REDACTED] detasking records was performed for the date range February 2009 to March 2010.

(b)(3)-P.L. 86-36

(S//SI//REL TO USA, FVEY)

## (U//FOUO) Detasked Selectors by Source and Type

(S//SI//REL TO USA, FVEY)

| Source                         | Type | \$702 Selector Type | Description                                       | Time Frame                  | No. of Detasked Selectors |
|--------------------------------|------|---------------------|---|-----------------------------|---------------------------|
| SV4 PAA/FAA Incidents database |      |                     | Compliance-related detaskings since July 2008     | July 2008 to March 2010     |                           |
| SV4 PAA/FAA Incidents database |      |                     | Compliance-related detaskings since July 2008     | July 2008 to March 2010     |                           |
| SV4 PAA/FAA Incidents database |      |                     | Compliance-related detaskings since July 2008     | July 2008 to March 2010     |                           |
| SV4 PAA/FAA Incidents database |      |                     | Compliance-related detaskings since July 2008     | July 2008 to March 2010     |                           |
| D [redacted] detasking record  |      |                     | Compliance-related detaskings since February 2009 | February 2009 to March 2010 |                           |
| D [redacted] detasking record  |      |                     | Compliance-related detaskings since February 2009 | February 2009 to March 2010 |                           |
| Total                          |      |                     |   |                             |                           |

(S//SI//REL TO USA, FVEY)

(b)(3)-P.L. 86-366

(b)(1)  
(b)(3)-P.L. 86-366

## (U) Audit Sample for Gap Analysis

(b)(1)  
(b)(3)-P.L. 86-366  
(b)(1)-P.L. 86-366

(S//SI//REL TO USA, FVEY) The focus of our gap analysis was on FAAL [redacted] selectors that were detasked for collection for compliance reasons under the [redacted] certification from February 2009 to March 2010. We concentrated on the selectors from the [redacted] certification because of the significance of the FAAL \$702 collection, including the number of FAAL \$702 taskings, and the key role it plays in [redacted] SIGINT production. We also based our decisions regarding the time frame for review and the focus on [redacted] selectors on the availability of records necessary to conduct the analysis, and the majority of the \$702 detaskings were [redacted]. There were [redacted] detasked [redacted] selectors. We were unable to conduct an analysis of [redacted] selectors because of a lack of traffic or tasking information or both.

(S//SI//REL TO USA, FVEY) Our analysis covered both time gaps (gaps in coverage in days) and collection coverage gaps (projected missed collection as a result of the loss of coverage) for the [redacted] [redacted] selectors.

(b)(1))

(b)(3)-P.L. 86-366

(S//SI//REL TO USA, FVEY)

| Database                       | Type | \$702 Selector Type | Selectors Reviewed<br>(February 2009 to March 2010) |  |  |
|--------------------------------|------|---------------------|---|--|--|
| SV4 PAA/FAA Incidents database |      |                     |   |  |  |
| D [redacted] detasking records |      |                     |   |  |  |
| Total                          |      |                     |   |  |  |

(b)(3)-P.L. 86-366

(U//FOUO) Records reviewed

(U//FOUO) To measure the extent of the gaps associated with detasked §702 selectors, we evaluated multiple sources of information. This information was requested from SV, [REDACTED]

[REDACTED] and the §2 [REDACTED] We also reviewed the following databases: [REDACTED]

(b)(3)-P.L.86-36

• (U//FOUO) §702 tasking history

(U//FOUO) [REDACTED] records were used to determine the dates of coverage for the selectors. The data included the dates the selectors were tasked and detasked in [REDACTED] for Executive Order 12333 and §702 coverage.

• (U//FOUO)

(U//FOUO) Data were requested from the [REDACTED] on the tasking and detasking of the selectors. This allowed us to draw a comparison between information in the SV4 PAA/FAA Incidents database and the tasking records from [REDACTED]. We also used the [REDACTED] data to determine the Effective Collection Priority of each of the selectors.

• (U//FOUO)

(U//FOUO) [REDACTED] data were requested for determination of the number of pieces of traffic, or "traffic hits," collected per day related to §702 [REDACTED]. This traffic allowed us to determine how active the selectors were in regard to traffic collected [REDACTED]. From this information, we were able to project the potential collection that was lost during gaps in coverage related to §702 compliance. It also provided us the ability to determine how [REDACTED]

(C)flf  
(b)(1)

(b)(3)-P.L. 86-36

(b)(3) 50 USC 3024(i)

• (U//FOUO) Purged records

(U//FOUO) Purge requests from SV4 to database managers were evaluated for records related to the group of [REDACTED] selectors in the [REDACTED] database. The purged records in effect represent a gap in collection coverage.

• (U//~~FOUO~~) §704/§705b tasking

(S//~~SHR/REL TO USA, FWBM~~) Reports were generated from [redacted] and records requested from SV regarding §704/§705b authorizations to determine if any of the [redacted] j detasked §702 selectors were subsequently approved under those authorizations.

D

(b)(3)-P.L. 86-36

(b)(1)  
(b)(3)-P.L. 86-36

(U) This page intentionally left blank.

**(U) APPENDIX C**

**(U) Full Text of Management Comments**

~~TOP SECRET//COMINT//NOFORN~~

## (U) SID and OGC Management Response

| <del>TOP SECRET//COMINT//NOFORN</del>  |  |                    |   |                   |   |
|--|--|--------------------|---|-------------------|---|
| SECURITY CLASSIFICATION<br><b>NSA STAFF PROCESSING FORM</b>  |  |                    |   |                   |   |
| <b>TO</b><br>OIG   | EXREG CONTROL NUMBER<br>2010-8956  | KCC CONTROL NUMBER |   |                   |   |
| <b>THRU</b><br>0-21-<br>SUBJECT  | <b>ACTION</b><br><input type="checkbox"/> APPROVAL<br><input checked="" type="checkbox"/> SIGNATURE<br><input checked="" type="checkbox"/> INFORMATION |                    |   |                   | EXREG SUSPENSE<br>15 Nov 2010<br>KCC SUSPENSE<br>ELEMENT SUSPENSE<br>ELEMENT SUSPENSE |
| (U// <del>FOUO</del> ) SID Response to Draft Audit Report on the FISA Amendments Act 702 Detasking Requirements  |  |                    |   |                   |   |
| <b>DISTRIBUTION:</b>   |  |                    |   |                   |   |
| <b>SUMMARY:</b>  |  |                    |   |                   |   |
| <b>PURPOSE:</b> (U// <del>FOUO</del> ) To provide the SID response to the draft report on FISA Amendments Act (FAA) 702 Detasking Requirements (AU-10-0023).   |  |                    |   |                   |   |
| <b>BACKGROUND:</b> (U// <del>FOUO</del> ) The Audit was initiated at the request of DIRNSA. The Audit objective was to document the circumstances and the extent of dropped SIGINT collection as a result of FAA 702 restrictions. The draft Audit report was provided to [REDACTED] |  |                    |   |                   |   |
| <b>DISCUSSION:</b> (U// <del>FOUO</del> ) The attached document (TAB 4) is the consolidated SID/S2 and OGC response to the subject report. The [REDACTED] deferred to [REDACTED] for their response to this tasker.  |  |                    |   |                   |   |
| b)(1)<br>(b)(3)-P.L. 86-36<br>(b)(3)-P.L. 86-36<br>(b)(3)-50 USC 3624(i)   |  |                    |   |                   |   |
| <i>This SPF may be downgraded and marked SECRET//COMINT//NOFORN upon removal of end(s).</i>  |  |                    |   |                   |   |
| COORDINATION/APPROVAL  |  |                    |   |                   |   |
| OFFICE   | NAME AND DATE  | SECURE PHONE       | OFFICE  | NAME AND DATE     | SECURE PHONE  |
| SID DIR  | [REDACTED]   | [REDACTED]         | [REDACTED]  | [REDACTED]        | [REDACTED]  |
| S2   | [REDACTED]   | 966-4335           | [REDACTED]  | (b)(3)-P.L. 86-36 | [REDACTED]  |
| S2   | [REDACTED]   | 966-4335           | [REDACTED]  | [REDACTED]        | [REDACTED]  |
| OCIC   | email/[REDACTED]   | 963-3121           | [REDACTED]  | [REDACTED]        | [REDACTED]  |
|  | [REDACTED]   | 963-4093           | [REDACTED]  | [REDACTED]        | [REDACTED]  |
| ORIGINATOR   | [REDACTED]   | ORG                | PHONE (SECURE)  | DATE PREPARED     |   |
|  | [REDACTED]   | S023               | 966-5590  | 11/15/2010        |   |
| <small>FORM A6796T REV FEB 2005 (Supersedes A6796 NOV 96 which is obsolete)<br/>NSN: 7540-01-0465</small>  |  |                    | <small>SECURITY CLASSIFICATION<br/>TOP SECRET//COMINT//NOFORN</small> |                   |   |
| <small>Derived From: NSA/CSSM 1-52<br/>Dated: 20070108<br/>Declassify On: 20020100</small>   |  |                    | <small>TOP SECRET//COMINT//NOFORN</small>                             |                   |   |

~~TOP SECRET//COMINT//NOFORN~~

I. (U) SUMMARY

(U//FOUO) As requested, this correspondence provides the Office of [redacted] and Office of General Counsel's (OGC) statements of [redacted] (b)(3)-P.L. 86-36 concurrence (or non-concurrence) with the recommendation contained in the Office of Inspector General's (OIG's) draft audit report on the transitioning of NSA encounters with targets of Foreign Intelligence Surveillance Act (FISA) Amendments Act (FAA) §702 collection must be de-tasked from this collection authority. This memorandum also provides OIG with the results of [redacted] and OGC's review of the draft report for factual accuracy.

II. (U) CONCURRENCE WITH RECOMMENDATION

(TS//SI//NF) Recommendation : Establish a process for NSA [redacted] coverage for accounts de-tasked from FAA 702 collection.

(b)(1)  
(b)(3)-P.L. 86-36  
(b)(3)-50 USC 3024(i)

(U) Lead Actionee: SID with OGC.

(U) Concur/Non-Concur & Estimated Completion Date: [redacted] and OGC concur with OIG's recommendation. Corrective action is underway and will be completed as soon as possible. [redacted] Successful completion within this timeframe is contingent upon direct involvement from SV and S1 as they are owners of mission components that are directly tied to the transition process.

(TS//SI//NF) Comment: Although there is a current process for the Signals Intelligence Directorate (SID) [redacted] coverage of targets of interest, OGC does not dispute OIG's substantive finding that the current process does not appear to be universally understood by SID's [redacted] personnel. In

response to this finding and recommendation, OGC and individuals from SID, to include [redacted] personnel, are working on improving the current process [redacted]

[redacted] coverage of [redacted] targets that must be dropped from FAA 702 collection. OGC and SID [redacted] personnel have already initiated discussions to

establish a clearer process for NSA [redacted] coverage for selectors de-tasked from FAA 702 collection. OGC and [redacted] personnel have begun drafting a comprehensive standard operating procedure (SOP) for analysts to follow when

[redacted] as appropriate. The SOP will also include a quick reference guide and checklist for analysts. OGC will engage with the Department of Justice (DoJ) [redacted] as

(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36

necessary to ensure that the new process addresses OIG's findings and recommendation.

(b)(1) (b)(3)-P.L. 86-36 (TS//SI//NF) In the short term, [ ] has initiated a series of training sessions for [ ] (b)(3)-P.L. 86-36 (b)(3)-50 USC 3024(i) members of the division and branch leadership teams to raise awareness of the process [ ] The purpose of the training is to establish branch and division level Points of Contact (POCs) who will be able to assist analysts through the [ ] process. Additional Video Teleconferencing Center (VTC) sessions will be scheduled to include the extended enterprise.

(b)(3)-P.L. 86-36

(TS//SI//NF) Finally, an e-mail alias has been created that includes technical and policy experts in [ ] The purpose of this group is to assist the division and branch POCs as they work with the analysts on the [ ] process. Members of the group will also ensure that timely resolution is reached for selectors de-tasked from FAA 702.

### III. (U) [ ] REVIEW FOR FACTUAL ACCURACY

(b)(3)-P.L. 86-36

(U//FOUO) OIG Comment: The OIG does not agree with the [ ] that all suggested changes were due to inaccuracies or misleading statements. In most cases, these suggested changes were based on [ ] interpretations of the report and new information. We made the appropriate changes to update and clarify areas of the report.

(S//SI//NF) The following lists areas of the report where [ ] identified factual inaccuracies or misleading statements that should be corrected in the final version of OIG's report on the [ ] gap NSA encounters when targets of FAA 702 collection must be de-tasked from this collection authority. These factual inaccuracies do not affect [ ] concurrence with the report's recommendation that SID and OGC establish a new process!

[ ] targets that must be dropped from FAA 702 collection. The following constitutes [ ] specific suggested corrections:

(U) Correction 1

(b)(3)-P.L. 86-36

(b)(1)

(b)(3)-P.L. 86-36

(b)(3)-50 USC 3024(i)

(S//SI//NF) Highlights Section (page i): On page "i" in the "Highlights" section, the report contains a section that says [ ]

-(S//SI//NF) Comment: This statement implies that NSA would have been able to obtain probable cause on all of those selectors and would have been able to transition to another authority. Believe we should clarify that we cannot transition all selectors in all circumstances.

(U) Correction 22

(b)(3)-P.L. 86-36

-(S//SI//NF) Gap in [redacted] coverage Exist (page 5): Under the FINDINGS (top of the page), it states "...the Agency has experienced [redacted] of coverage gaps when transitioning from FAA702 to another authority."

-(S//SI//NF) Comment: This statement implies that NSA should be able to transition to another authority in all instances. This is not the case. Believe we should clarify that we cannot transition all selectors in all circumstances. While the need for a "higher legal standard" is mentioned on the bottom of page 6, believe we need to be up front with the fact that some selectors will not transition.

(U) Correction 33

-(S//SI//NF) Effective Collection Priority (ECP) (page 8): This section states that the average ECP was 2.52 indicating that the average ECP was 2.52, indicating that these selectors are of high priority."

-(S//SI//NF) Comment: Believe we need to add context to this statement. We would imagine that most if not all [redacted] has an (b)(3)-P.L. 86-36 ECP that falls into the 1-3 range. Probably all [redacted] selectors are of high priority based on the ECP.

(U) Correction 44

-(S//SI//NF) Selectors not retasked (page 11): The table at the top of the page indicates that [redacted] (b)(1)  
(b)(3)-P.L. 86-36

-(S//SI//NF) Comment: We think it is important to add a footer that indicates that the analysts were told that they did NOT have to perform thorough research to try to recall why the selector was not retasked. Below is an excerpt from an email exchange between DIA and [redacted] indicating that the analyst did not have to perform research if they did not remember why the selector was not retasked.

(TS//SI//NF) We agree with your assertion that the analysis simply notes that they do not recall what happened to the selectors if they cannot remember. Our intention was not to require people to spend hours trying to recall information to answer our survey, which is why there is a "don't recall" option in the first question. (b)(1)

(b)(3)-P.L. 86-36

(b)(3)-50 USC 3024(i))

(U) Correction<sup>55</sup>

(TS//SI//NF) [REDACTED]

[REDACTED]

[REDACTED]

(U) Correction<sup>66</sup>

(TS//SI//NF) Need for consistent process (page 11): The document states that,

(b)(1))

(b)(3)-P.L. 86-36

(b)(3)-50 USC 3024(i))

(TS//SI//NF) Comment: We think it is important to note that some selectors will take longer to transition compared to others based on the circumstances. The probable cause standard is higher than the standard associated FAA 702 tasking. This statement implies that less bold data always be able to transition quickly. It may take time and a lot of back and forth between [REDACTED] before we (b)(3)-P.L. 86-36 reach the probable cause standard. We realize this is addressed in the Case Studies on page 13 but we think it should be stated up front.

(U) Correction<sup>77</sup>

(S//SI//REL) Footnote 3 (page 14): States that [REDACTED]

(b)(1)-P.L. 86-36

(TS//SI//NF) Comment: [REDACTED]

(b)(1)

(b)(3)-P.L. 86-36

b)(3)-P.L. 86-36

(U) Correction 88

~~(TS//SI//NF)~~ First Paragraph (page 15): "The analysts also may not have been

(b)(1)  
(b)(3)-P.L. 86-36  
(b)(3)-50 USC 3024(i)

-4P-

~~(TS//SI//NF)~~ Comment:

(U) Correction 99

~~(TS//SI//NF)~~ Action Taken (page 18): This section discusses the new procedures which are supposed to provide relief on some [redacted] scenarios.

(b)(1)  
(b)(3)-P.L. 86-36

~~(TS//SI//NF)~~ Comment: Unfortunately, [redacted] provisions were removed from the new procedures so we will not see any [redacted] relief based on the new procedures. OGGC would have detailed shortly what occurred and where we stand.

(b)(1)  
(b)(3)-P.L. 86-36

III. (U) OGC - REVIEW FOR FACTUAL ACCURACY

~~(U//FOUO)~~ OIG Comment: The OIG does not agree with the OGC that all suggested changes were due to inaccuracies or misleading statements. In most cases, these suggested changes were based on OGC's interpretation of the report and new information. We made the appropriate changes to update and clarify areas of the report.

~~(S//SI//NF)~~ The following lists areas of the report where OGC identified factual inaccuracies that should be corrected in the final version of OIG's report to the transition gap. NSA encounters when targets of FAA 702 collection must be de-tasked from this collection authority. These factual inaccuracies do not affect OGC's concurrence with the report's recommendation that SID and OGC establish a new process [redacted] targets that must be dropped from FAA 702 collection. The following constitutes OGC's specific suggested corrections:

(b)(1)  
(b)(3)-P.L. 86-36  
(b)(3)-50 USC 3024(i)

(U) Correction 11

(b)(1)  
(b)(3)-P.L. 86-36

~~(S//SI//NF)~~ **Highlights Section** (page i): On-page "i" in the "Highlights" section, the report contains a sentence that says the issue of a [redacted]  
[redacted] is currently under review by DoJ. This statement is factually incorrect. In July 2010, DoJ attempted to persuade the Foreign Intelligence Surveillance Court (FISC) to allow tasking to continue under one version of the [redacted] but the FISC refused to accept the proposed change to NSA's FAA targeting and minimization procedures that the Government proposed to address this problem. OGC's understanding is that the FISC concluded such a change would conflict with statutory restrictions contained in the FAA legislation itself. Therefore, DoJ is no longer reviewing this issue in the manner mentioned in the draft report. Instead, DoJ is reviewing two different draft legislative proposals that attempt to close the transition gap. One proposal was drafted by NSA and the other proposal was prepared by DoJ's National Security Division. [redacted]

(U) Correction 22

(b)(1)  
(b)(3)-P.L. 86-36

~~(S//SI//NF)~~ **Introduction:** On page 2, the "Introduction" section of the draft report contains the following sentence:

(b)(1)f.....~~(S//SI//NF)~~ "Under FISC docket number [redacted] (known as the Raw Take (b)(3)-P.L. 86-36 Sharing Order) dated July 2002, NSA is able to receive FBI FISA collection." (b)(3)-50 USC 3024(i)

(U) As drafted, this sentence is factually inaccurate. This sentence should be revised to read:

~~(S//SI//NF)~~ "Under FISC docket number [redacted] (known as the Raw Take Sharing Order) dated July 2002, NSA is able to receive most FBI FISA collection directed against the FBI's counterterrorism targets."

## (U) Correction 33

(b)(3)-P.L.866386

(S//SI//NF) Finding that Gaps in [ ] Target Coverage Exist: Page 6 of this section of the draft report contains the following sentence:

(S//SI//NF) "To avoid a break in coverage, other authorities must be sought if the target remains of interest and is an agent of a foreign power (§704, §705b, and/or FBI FISA)."

(S//SI//NF) This sentence is inaccurate as drafted since it implies that the listed authorities are the only possible authorities available to resume coverage. The sentence should be revised to read:

(S//SI//NF) "To avoid a break in coverage, other authorities must be sought if the target remains of interest and is an agent of a foreign power (e.g., §704, §705b, FBI FISA, etc.)."

## (U) Correction 44

(b)(3)-P.L.866386

(S//SI//NF) Finding that Gaps in [ ] Target Coverage Exist: Page 6 of this section of the draft report contains the following statement:

(S//SI//NF) "For non-FAM §702 coverage, a higher legal standard, individualized probable cause, is required to secure a FISA order. [ ]

(S//SI//NF) Although the statement is accurate as drafted, for completeness OIG may wish to note that, in some cases, the Government may simply not be able to assemble facts sufficient to satisfy the probable cause standard.

(b)(1)  
(b)(3)-P.L.866386

## (U) Correction 55

(S//SI//NF) Discussion of lack of process [ ] On pages 15 to 16 of this section of the draft report, there is a discussion of the delay experienced in regaining coverage of selectors associated with [ ].

[ ] Indeed the report says

NSA had to de-task the account once the Agency learned that [REDACTED]

(b)(1)  
(b)(3)-P.L. 86-36  
(b)(3)-50 USC 3024

(U) Correction<sup>66</sup>

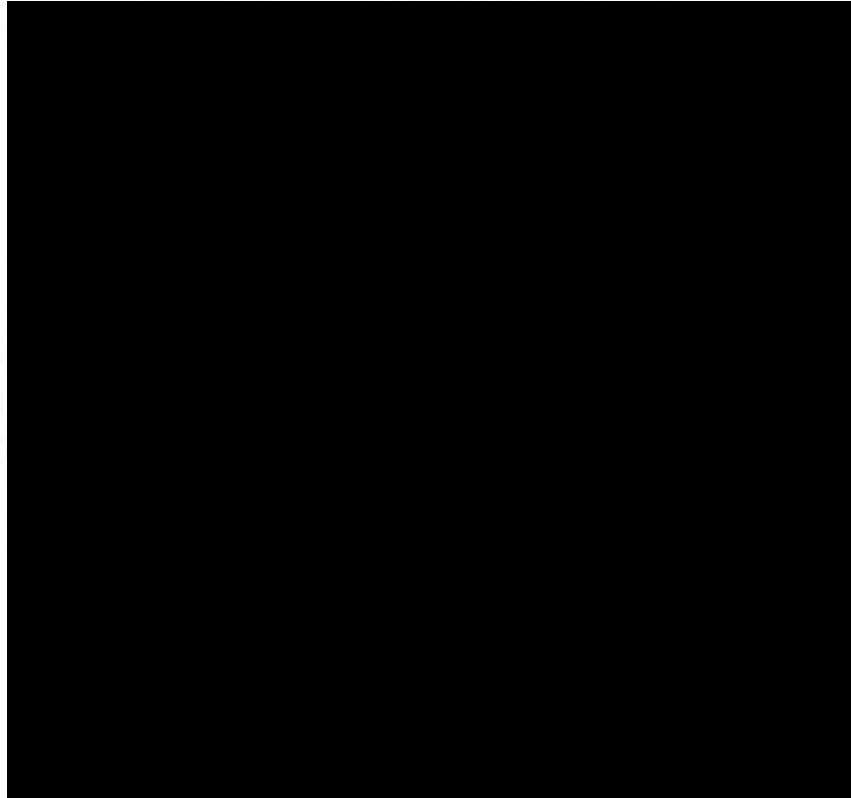
~~(S//SI//NF)~~ Discussion of "Strict guidance on de-tasking": On pages 17 to 18, the draft report states that DoJ and OGC have provided "strict guidance" to de-task [REDACTED]. Although accurate, as drafted the report implies that DoJ and OGC have discretion to alter the guidance. Therefore, the draft report's discussion of the legal advice provided by DoJ and OGC on de-tasking of [REDACTED] is extremely misleading. Although this section of the draft report notes that the FISC has expressed "concern" about the modifications the Government proposed [REDACTED] to NSA's FAA 702 targeting and minimization procedures, the report fails to note that the Court's concern was with the [REDACTED] issue. OGC's understanding is that the Court concluded that even the modest changes proposed [REDACTED] to address one aspect of the [REDACTED] were incompatible with the current statutory framework. Moreover, for completeness, the report should also note that, even if the statutory language is changed, there may be Fourth Amendment problems with maintaining electronic surveillance of a U.S. person or a person located inside the United States on anything less than a formal probable cause determination.

~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~

**NATIONAL SECURITY AGENCY/CENTRAL SECURITY  
SERVICE**

Further dissemination of this report outside NSA is  
PROHIBITED without the approval of the Inspector  
General.



**(U) Report on the Special Study: Assessment of  
Management Controls Over FAA §7022  
ST-11-0009**

**Revised and Reissued 29 March 2013**

**(b)(3)-P.L. 86-36**

Classified By: [redacted]

Derived From: NSA/CSSM11522

Dated: 20070108

Declassify On: 28388301

Approved for Release by NSA on 02-11-2016. FOIA Case# 80120 {litigation}

TOP SECRET//SI//NOFORN

**(U) OFFICE OF THE INSPECTOR GENERAL**

(U) Chartered by the NSA Director and by statute, the Office of the Inspector General conducts audits, investigations, inspections, and special studies. Its mission is to ensure the integrity, efficiency, and effectiveness of NSA operations, provide intelligence oversight, protect against fraud, waste, and mismanagement of resources by the Agency and its affiliates, and ensure that NSA activities comply with the law. The OIG also serves as an ombudsman, assisting NSA/CSSS employees, civilian and military.

**(U) AUDITS**

(U) The audit function provides independent assessments of programs and organizations. Performance audits evaluate the effectiveness and efficiency of entities and programs and their internal controls. Financial audits determine the accuracy of the Agency's financial statements. All audits are conducted in accordance with standards established by the Comptroller General of the United States.

**(U) INVESTIGATIONS**

(U) The OIG administers a system for receiving complaints (including anonymous tips) about fraud, waste, and mismanagement. Investigations may be initiated in response to those complaints, at the request of management, or the result of irregularities that surface during inspections and audits, or at the initiative of the Inspector General.

**(U) INTELLIGENCE OVERSIGHT**

(U) Intelligence oversight is designed to insure that Agency intelligence functions comply with federal law, executive order, and NSA policies. The IO mission is grounded in Executive Order 12333, which establishes broad principles under which IC components must accomplish their missions.

**(U) FIELD INSPECTIONS**

(U) Inspections are organizational reviews that assess the effectiveness and efficiency of Agency components. The Field Inspections Division collaborates with Inspector General of the Service Cryptologic Element and the Field Entities to jointly inspect established cryptographic facilities.

**OFFICE OF THE INSPECTOR GENERAL  
NATIONAL SECURITY AGENCY  
CENTRAL SECURITY SERVICE**

29 March 2013

IG-11526-13

**TO: DISTRIBUTION**

**SUBJECT: (U) Revised Report on the Special Study: Assessment of Management Controls Over FAA §702 (ST-11-00099)-ACTION MEMORANDUM**

1. (U//~~FOUO~~) This revised report summarizes the results of our special study of management controls that ensure compliance with Section 702 of the Foreign Intelligence Surveillance Act (FISA) Amendments Act of 2008 (FAA §702) and the Targeting and Minimization Procedures associated with the 2011 Certifications. It reflects changes made based upon additional information provided subsequent to the release of the original report on 8 November 2012. The report documents our analysis, findings, and recommendations for improvement. It also notes other areas that merit attention.
  2. (U//~~FOUO~~) In accordance with NSA/CSSS Policy 1-60, NSA/CSSS *Office of the Inspector General*, and IG-11358-12, *Follow-up Procedures for OIG Report Recommendations*, actions on OIG recommendations are subject to monitoring and follow-up until completion. Consequently, we ask that you provide a written report concerning each OPEN recommendation in the following circumstances: when your action plan has been fully implemented or has changed or if the recommendation is no longer valid. The report should provide sufficient information to show that corrective actions have been completed. If a planned action will not be completed by the target date, please state the reason for the delay and give a revised completion date. Reports should be sent to [REDACTED] Follow-Up Program Manager, at e-mail DL D1\_Followup (ALIAS) D1.

3. (U) We appreciate the courtesy and cooperation extended to our staff throughout the special study. For additional information, please contact [REDACTED] on 963-1422(s) or via e-mail at [REDACTED]

(b)(3)-P.L. 86-36

*a>S~A f*  
George Ellard  
DR. GEORGE ELLARD  
Inspector General

(S//NF) DISTRIBUTION:

DIRNSA  
SID (T. Shea)  
NTOC (R. Ledgett)  
TD (L. Andersson)  
DOC (J. DeLong)  
OGC (R. De)  
ADET (J. Majors\$)

cc: Exec DIR (F. Fleiseth)

CoS (E. Brooks)  
SID DDIR (R. Moultrie)

DDCR

DDAP

DDDA

SID CoS

Chief, SV

DL SIDIGLIAISON

DL ntocreg

DL d\_comply\_tasker

DL REGISTRY

DL d\_gc\_tasker

(b)(3)-P.L. 86-36

(b)(6)

gt

IG

D1

D11

D12

D13

D14

**(U) TABLE OF CONTENTS**

|   |            |
|---|------------|
| <b>(U) EXECUTIVE SUMMARY .....</b>  | <b>iii</b> |
| <b>I. (U) INTRODUCTION .....</b>  | <b>1</b>   |
| <b>II. (U//FOUO) FINDINGS RESOLVED DURING THE REVIEW.....</b>   | <b>11</b>  |
| <b>III. (U//FOUO) FINDINGS AND RECOMMENDATIONS .....</b>  | <b>13</b>  |
| (U//FOUO) FINDING ONE: PERFORMANCE STANDARDS, PERFORMANCE METRICS, AND<br>COMPLIANCE ENFORCEMENT MEASURES FOR TARGETING AND MINIMIZATION<br>PROCEDURES ARE INCOMPLETE ..... | 13         |
| (U//FOUO) FINDING TWO: CERTAIN FAA §702 SELECTORS [REDACTED] .....  | 19         |
| (U//FOUO) FINDING THREE: OVERSIGHT REQUIREMENTS OF FAA §702 TARGETING<br>PROCEDURES AND NSA POLICY ARE NOT FULLY ADDRESSED .....  | 21         |
| (U//FOUO) FINDING FOUR: SOME DOCUMENTATION SUPPORTING FAA §702<br>RESPONSIBILITIES HAS NOT BEEN KEPT UP-TO-DATE AND PROCURES REORGANIZATION<br>ACROSS NSA WEB PAGES .....   | 25         |
| (U//FOUO) FINDING FIVE: INCREASED AUTOMATION OF PROCESSES SUPPORTING<br>FAA §702 IS NEEDED TO ENSURE COMPLIANCE AND REDUCE ERRORS .....                                     | 29         |
| (U//FOUO) FINDING SIX: THE FAA §702 CURRICULUM NEEDS TO BE UPDATED AND THE<br>TRAINING REQUIREMENT ENFORCED .....   | 35         |
| <b>IV. (U) OBSERVATIONS.....</b>  | <b>39</b>  |
| <b>V. (U//FOUO) SUMMARY OF RECOMMENDATIONS .....</b>  | <b>41</b>  |
| <b>VI. (U) ABBREVIATIONS AND ORGANIZATIONS .....</b>  | <b>45</b>  |

**APPENDIX A: (U) About the Study**

**APPENDIX B: (U) Control Requirements and Management Controls**

**APPENDIX C: (U) Full Text of Management Responses**

(U) This page intentionally left blank.

~~TOP SECRET//SI//NOFORN~~

## (U) EXECUTIVE SUMMARY

### (U) Overview

(S//SI//NF) The National Security Agency/Central Security Service (NSA/CSS) conducts activities under the authority of Section 702 of the Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008 (FAA §702), a key source of information on foreign targets. Since FAA's inception, reporting based on FAA §702 collection has grown from an average of [redacted] reports per month to more than [redacted]. FAA §702 reports are sourced from collection obtained with the assistance of U.S. communications service providers. The majority of the collection [redacted] [redacted] is from Internet Service Providers (PRISM traffic), and the remainder (telephony and upstream Internet traffic) is obtained from [redacted] [redacted] the Internet backbone. (b)(1) (b)(3)-P.L. 86-36

(U//FOUO) For the Agency to retain this important tool in support of its mission, it must ensure compliance with FAA §702. NSA/CSS has implemented policies and control procedures, including training, access control, multiple levels of review, and oversight. This system of controls is designed to provide reasonable assurance of compliance with the statute and FAA §702 targeting and minimization procedures that form the basis for the affidavits made by the NSA Director concerning the Agency's use of the authority.

(U//FOUO) The findings represent improvements needed to the overall control environment in which the FAA §702 authority is used. In a later review, the Office of the Inspector General will conduct compliance and substantive testing to draw conclusions on the efficacy of the management controls.

(b)(1)

(b)(3)-P.L. 86-36

(b)(3)-50 USC 3024(i)

### (U) Highlights

(U//FOUO) Although the OIG did not identify areas of non-compliance with the targeting and minimization procedures, we identified six areas in which controls over compliance with FAA §702 should be improved:

- (U//FOUO) **Assessment of performance against compliance standards**  
Establishing accountability for compliance requires clear performance standards, measurement of actual performance against those standards, reporting results, and implementation of corrective action. These processes are not fully developed.

~~-TOP SECRET//SI//NOFORN-~~

(b)(1) [REDACTED]  
(b)(3)-P.L. 86-36  
(b)(3)-50 USC 3024(i)

- ~~(TS//SI//NF)~~ [REDACTED]

- ~~(TS//SI//NF)~~ **Dissemination process**  
A review of FAA §702 -sourced serialized dissemination does not include steps to verify that, when MCTs were used to support what is being disseminated, the multiple communications transaction (MCT) documentation required was prepared in accordance with the minimization procedures.

- ~~(U//FOUO)~~ **Documentation deficiencies**

Some internal Standard Operating Procedures and other internal FAA §702 guidance have not been kept up to date and require reorganization by subject across internal NSA web pages.

- ~~(U//FOUO)~~ [REDACTED]

(b)(3)-P.L. 86-36

[REDACTED] would improve purge execution, training compliance, and production of compliance alerts.

- ~~(U//FOUO)~~ **Training update and enforcement**

Adjudicators (personnel responsible for approving targeting requests) do not have a documented, standardized version of their training for reference. In addition to the initial FAA §702 training required before accessing FAA data, analysts are now required to take a new FAA §702 applications course on compliant targeting requests and targeting maintenance. However, the requirement for the applications course is not yet enforced.

#### **(U) Management Action**

~~(U//FOUO)~~ Signals Intelligence Directorate personnel agreed with the Inspector General recommendations, and the planned actions meet the intent of the recommendations.

~~-TOP SECRET//SI//NOFORN-~~

## I. (U) INTRODUCTION

### (U) Background

#### (U) Sources of Section 702 Foreign Intelligence Surveillance Act (FISA) Amendments Act of 2008 (FAA §702) collection

(b)(3)-P.L. 86-36

(TS//SI//NF) FAA §702 data is composed of Digital Network Intelligence (DNI) and Dialed Number Recognition (DNR) data. DNI is Signals Intelligence (SIGINT) received from Internet Service Providers (ISPs) with the assistance of the Federal Bureau of Investigation (FBI) (the PRISM program), and from [REDACTED] (upstream collection). Analysts submitting

(b)(1)  
(b)(3)-P.L. 86-36

FAA §702 tasking can [REDACTED]. DNR data is SIGINT obtained via intercept of the telephone network. NSA has the authority to acquire communications to, from, or, in the case of DNI collection from [REDACTED] about tasked selectors.

#### (U) Requirements of FAA §702

(S//NF) The target of collection must be a non-US person (USP) who is reasonably believed to be located outside the United States and possesses, is expected to receive, and/or is likely to communicate foreign intelligence

[REDACTED] 1 FAA §702 Certifications:

(b)(1)  
(b)(3)-P.L. 86-36  
(b)(3)-50 USC 3024(i)

(S//NF) FAA §702 requires the Attorney General to adopt targeting and minimization procedures in support of the statute. The targeting and minimization procedures are documented in each Certification. DIRNSA's affidavit for each certification provides information regarding how the Government will implement those procedures and states that:

(S//NF)

(b)(1)

(b)(3)-P.L. 86-36

(b)(3)-50 USC 302

- Reasonable procedures are in place to ensure that acquisition under the Certification is limited to targeting non-USPs reasonably believed to be located outside the United States.
- Targeting procedures are reasonably designed to prevent the intentional acquisition of domestic communications.<sup>2</sup>
- Acquisition is for the purpose of obtaining foreign intelligence information within the scope of each Certification.
- NSA will follow specific minimization procedures.
- NSA may provide the Central Intelligence Agency (CIA) and the FBI unminimized communications acquired through this authority.

**(U) Independent measure of compliance performance**

~~(S//NF)~~ The Agency's compliance with FAA §702 is subject to bi-monthly review by the Department of Justice (DOJ) and the Office of the Director of National Intelligence (ODNI), who review disseminations, queries of U.S. person identifiers, compliance incidents, and the targeting requests for all new and retained selectors for the period as well as the supporting information for a sample of the selectors. These entities have reported a very small number of errors.

---

**(U) Objectives and Scope of Review**

~~(U) (FOUO)~~ The objective of the OIG review was to assess the adequacy of management controls to ensure reasonable compliance with FAA §702. This analysis was based on review of published and draft guidance and certain controls in systems supporting application of the authority. We also interviewed managers and analysts responsible for targeting, approval, and oversight subject to FAA §702 requirements. Testing of the controls identified will be the subject of a later review.

---

**(U) Standards of Internal Control**

~~(U)~~ We assessed management controls against the Government Accountability Office's *Standards for Internal Control in the Federal Government*, November 1999, which presents the five standards that define the minimum level of quality acceptable for management control in government: Control Environment, Risk Assessment, Control Activities, Information and Communications, and Monitoring.

~~(U)~~ Internal control, or management control, comprises the plans, methods, and procedures used to meet missions, goals, and objectives. It provides

---

~~(S//NF)~~ Domestic communications, according to Section 22 of the FAA §702 Minimization Procedures, are all communications other than foreign communications, including those in which the sender and all intended recipients are reasonably believed to be located in the United States at the time of acquisition. Foreign communications must have at least one communicant outside the United States.

~~TOP SECRET//SI//NOFORN~~

reasonable assurance that an entity is effective and efficient in its operations, reliable in its reporting, and compliant with laws and regulations. NSA/CSSS Policy 7-33, *Managers' Internal Control Program*, 14 February 2012, advises that evaluations of internal control consider the requirements outlined by the GAO standards. The Office of the Inspector General (OIG) evaluates management control against the standards.

### (U) Targeting and Minimization Procedures: Basis for Compliance

#### (U) Targeting

~~(S//SI//NF)~~ The targeting procedures specify that NSA will make a determination about "whether a person is a non-United States person reasonably believed to be outside the United States in light of the totality of the circumstances based on the information available with respect to that [redacted]

(b)(1) [redacted] With respect to the foreign intelligence purpose for the targeting, the procedures require NSA to assess "whether the target possesses and/or is likely to communicate foreign intelligence information concerning a foreign power or foreign territory...." With respect to documentation, analysts who request tasking will document in the tasking database a citation or citations to the information that led them to reasonably believe that a targeted person is located outside the United States" as well as "identify the foreign power [redacted] about which they expect to obtain foreign intelligence information pursuant to the proposed targeting".

~~(S//SI//NF)~~ The submitted targeting request is then subject to an adjudication review by specially trained personnel [redacted]

(b)(1)  
(b)(3)-P.L.866366  
(b)(3)-50 USE 30241

1

~~(S//SI//NF)~~ **Obligation to review target status** Once collection begins, analysts are responsible for conducting "post-targeting analysis to detect those occasions when a person who when targeted was reasonably believed to be located outside the United States has since entered the United States, and...enable NSA to take steps to prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of acquisition to be located in the United States, or the intentional targeting of a person who is inside the United States," per the targeting procedures. NSA's *Guidance to Analysts on Obligation to Review Data Under...the FISA Amendments Act* (OTR Guidance), states that, after tasking, "analysts are required to verify the foreignness and nature of the target [redacted]" The OTR Guidance states that the targeting analyst must perform initial target verification within five business days of first receipt of data, verifying that the:

- User of the selector is the intended foreign intelligence target,

(b)(1)  
(b)(3)-P.L.866366

~~TOP SECRET//SI//NOFORN~~

- Target remains appropriate under the Certification cited in tasking, and
- Target remains outside the United States and/or there is no information to indicate that the target is inside the United States.

~~(S//NF)~~ The On-Going Target Review section of the OTR Guidance states that analysts must [REDACTED] to uphold that there has been no change in the target's status that would require adjustment to maintain NSA's compliance. At least every 30 days...the review should confirm that the:

(b)(1)  
(b)(3)-P.L.86306

- Selector remains associated with the intended target,
- Target remains appropriate to the Certification cited,
- Target remains outside the United States and/or there is no information to indicate that the target is inside the United States, and
- Type of data being obtained is not routinely of a type that is subject to immediate destruction requirements (i.e., domestic communications).

~~(S//NF)~~ Information that demonstrates a change in any of these factors might require detasking the selector, destroying or otherwise handling collected traffic in accordance with the minimization procedures, and notice to the Agency's overseers

#### **(U) Oversight and reporting**

~~(U//FOUO)~~ The Agency must:

- Train those targeting and those approving targeting or accessing FAA §702 information ;
- Ensure that FAA §702 raw traffic is stored only in authorized repositories and is accessible only to those who have had the proper training ; and
- Conduct spot-checks of targeting decisions, intelligence dissemination, and queries of data repositories for compliance.

#### **(U) Minimization**

~~(U//FOUO)~~ The minimization procedures are designed to protect USP information during acquisition, processing, retention, and dissemination of information obtained by targeting non-USPs reasonably believed to be located outside the United States. They require that the Agency ensure that:

- Acquisition is conducted in a manner designed, to the greatest extent feasible, to minimize the acquisition of information not relevant to the authorized purpose of the acquisition;
- Personnel...exercise reasonable judgment in determining whether information acquired must be minimized and...destroy inadvertently

~~TOP SECRET//SI//NF//ORI~~

acquired communications of or concerning a USP at the earliest practicable point in the processing cycle [unless the data can be retained under exception provisions detailed in the minimization procedures]; and

- Report(s) based on communications of or concerning a USP may be disseminated... if the identity of the USP is deleted and a generic term or symbol is substituted so that the information cannot reasonably be connected with an identifiable USP. Otherwise, dissemination of intelligence reports based on communication of or concerning a USP may be made to a recipient requiring the identity of such person only for the performance of official duties but only if meeting [certain] criteria.

## **(U) Control Environment**

---

### **(U) Reliance on manual controls**

(U//~~FOUO~~) A significant number of the procedures and controls established to ensure compliance with FAA §702 and NSA's count approved targeting and minimization procedures are manual. Thus, training, supervisory reviews, and oversight are critical elements of the control structure. Modifications to the systems relied on for targeting, collection, and processing continue to:

- Improve the ability to purge information when required,
- Identify and prevent instances of over-collection, and
- Improve efficacy and efficiency of processing and oversight.

### **(U//~~FOUO~~) Realignment of responsibility**

(U) SID has restructured operations to better manage FAA §702 processing and compliance.

- (S//SI//NF) [REDACTED] assumed responsibility for adjudicating FAA §702 [REDACTED]
- (S//NF) [REDACTED]
- (U//~~FOUO~~) S2 Mission and Compliance performs functions supporting use of the authority, as well as additional oversight of FAA §702 processing and compliance (SV continues to perform much of the direct oversight of targeting.) [REDACTED] assumed responsibility from SV for: [REDACTED]

(b)(3)-P.L.88636

~~TOP SECRET//SI//NOFORN~~

- o Execution of purges related to FAA §702 incidents (removal from data repositories of records ineligible for retention under the authority),
- o Implementation of a purge adjudication process to better ensure completeness of purges,
- o Development of processes and tools to enhance compliance while reducing the burden on analysts,
- o Training and oversight of targeting adjudicators, and
- o Preparation of additional management measures, including metrics, to improve accountability.

**(U) Continued process improvement**

~~(TS//SI//NF)~~ The Agency has undertaken several reviews of NSA systems and processes, as well as the data acquired from communications providers and other Agency sources under FAA §702 authority, in response to compliance incidents and questions raised by the Foreign Intelligence Surveillance Court (FISC). These reviews and other efforts to improve compliance and efficiency of operations have resulted in several changes to the processes and controls supporting the Agency's use of the authority.

~~(S//NF)~~ SID continues to take steps to improve FAA §702 compliance.

- In addition to FAA §702 training that focuses on legal requirements for use of the authority, a new course, "FAA702 Practical Applications," was released [REDACTED]

iii.13 J.P. 86-36

- SID continues to make changes to the targeting tool to support compliance and increase efficiency (see Findings Resolved During the Review, p. 9). [REDACTED] (b)(3)-P.L. 86-36
- SID completed the [REDACTED] Project to reduce errors in targeting requests. The most significant gaps identified included a lack of standardized feedback to targeting analysts for the reasons targeting requests failed approval [REDACTED]

[REDACTED] insufficient management reporting of denial targeting requests, and the need to increase accountability and compliance for targeting. Corrective actions, including standardized denial reasons, management reporting of denial metrics [REDACTED] [REDACTED] were implemented. These actions reduced average weekly denials of targeting requests by 24 percent [REDACTED]

[REDACTED] improved

~~TOP SECRET//SI//FOUO//R~~

compliance with required internal procedures for selector management, and reduced the risk of incidents.

### **(U) Definitions**

---

**(U) Annual Contribution Evaluation (ACE):** The Agency's performance management system based on established individual performance objectives and performance elements.

**(S//SI//NF) Adjudicators:** Personnel [REDACTED] (b)(3)-P.L. 86-36

[REDACTED] with responsibility for reviewing and approving FAA §702 targeting requests.

targeting requests.

(U//FOUO) [REDACTED]

which provides authorization attributes and access control services to enterprise programs and projects.

**(TS//SI//NF) Digital Network Intelligence (DNI):** SIGINT derived from communications involving Internet-based selectors [REDACTED]

(b)(1)

(b)(3)-P.L. 86-36

(b)(3)-50 USC 3024(i).

**(S//SI//NF) Dialed Number Recognition (DNR):** Collection process [REDACTED] from telephony systems.

**(U) Foreignness:** Assessment and documentation supporting the determination of reasonable belief that a target is not a United States person and is outside the United States.

**(U//FOUO) [REDACTED]** A corporate compliance tool that serves as a streamlined access control mechanism. [REDACTED] checks that individuals meet the necessary mission, training and clearance required for initial account access to SIGINT tools and databases.

(U//FOUO) [REDACTED]

(b)(3)-P.L. 86-36

**(U//FOUO) Master Purge List (MPL):** NSA's central record of SIGINT collection, including records derived from that collection, which NSA has purged. The list includes [REDACTED] that have been marked for purge or have been purged from [REDACTED] systems that are used in sourcing traffic for SIGINT reporting.

~~TOP SECRET//SI//FOUO//R~~

~~TOP SECRET//SI//NOFORN~~

(TS//SI//NF) **Multiple Communications Transaction (MCT):** Traffic containing more than one discrete communication. This traffic might contain discrete communications that are not to, from, or about tasklist selectors. Upstream collection might contain both discrete and MCT traffic and could include MCTs of non-targeted individuals that contain a tasklist selector.

(b)(3)-P.L. 86-36

(U//~~FOUO~~) [ ] A database repository that provides storage and retrieval of [ ] content. It is a raw SIGINT storage system.

[ ] NSA's primary storage, search, and retrieval mechanism for SIGINT [ ] It is a raw SIGINT storage system.

(TS//SI//NF) **PRISM:** PRISM refers to the portion of the FAAA 702 collection architecture where individual electronic communication service providers provide Internet communications [ ] that in general are hosted by the [ ]

(b)(1)

(b)(3)-P.L. 86-36

(b)(3)-50 USC 3024(i)

(b)(3)-P.L. 86-36

(U) **Purge:** The on-demand removal of data items, rendering them unrecoverable through standard mission data access mechanisms.

(U//~~FOUO~~) [ ]

(U//~~FOUO~~) **Raw SIGINT:** Any SIGINT acquired either as a result of search and development or as targeted collection operations against a foreign intelligence target before the information has been evaluated for foreign intelligence and minimized in accordance with the applicable set of minimization procedures.

(U//~~FOUO~~) [ ] A controlled information management system which is the authoritative data source for a given configuration managed data element and is governed in accordance with NSA/CSS Policy [ ]

(U//~~FOUO~~) [ ] A SID organization that leads planning and acquisition efforts for [ ] collection of intelligence.

(U//~~FOUO~~) [ ] : A SID initiative whose objective was to reduce targeting errors, thereby improving processing efficiency and compliance for FAAA §702 transactions.

~~-TOP SECRET//SI//NOFORN-~~

(b)(1) (b)(3)-P.L. 86-36 (b)(3)-50 USC 3024(i) -(TS//SI//NF) **Upstream Collection:** NSA's interception of Internet communications acquired from [REDACTED] located on the United States' Internet "backbone"; conducted with the assistance of electronic communications service providers who are located inside the United States and have been served with FAA §702 directives. This collection method [REDACTED] is distinguished from other FAA §702 DNI collection (PRISM)..

(b)(3)-P.L. 86-366

-(S//SI//NP) [REDACTED] The targeting tool for submitting DNI and DNR targeting compliant with FAA and other SIGINT authorities.

~~-TOP SECRET//SI//NOFORN-~~

~~TOP SECRET//SI//NOFORN~~

(U) This page intentionally left blank.

~~TOP SECRET//SI//NOFORN~~

## II. (U//FOUO) FINDINGS RESOLVED DURING THE REVIEW

### (U//FOUO) Incompatibility between Assigned Authorities [REDACTED]

#### and Compliance Controls for FAA §702 [REDACTED]

(S//NF) One of the primary NSA internal control mechanisms that ensure compliance with FAA §702 Targeting Procedures is the adjudication of targeting requests before tasking. This review confirms that the target and associated selector are tasked under the proper FAA §702 Certification, the target is not a USP, the target is outside the United States (foreign), and the determination of reasonable belief of foreignness is properly supported. An [REDACTED]

(b)(3)-P.L. 86-36

(U//FOUO) SV was aware of this gap between the NSA-required internal control and implementation of the internal control within the tool, and it was resolved [REDACTED]

(b)(3)-P.L. 86-36

### (S//NF) Increased Risk of FAA §702 Non-Compliance for [REDACTED] Tasked Selectors [REDACTED]

(S//NF) To support compliance with FAA §702, automated OTR notices that a required review of target communications is due are generated [REDACTED] and sent to analysts [REDACTED]

(b)(3)-P.L. 86-36

(S//NF) [REDACTED]

~~TOP SECRET//SI//NOFORN~~

(U) This page intentionally left blank.

~~TOP SECRET//SI//NOFORN~~

### III. (U//FOUO) FINDINGS AND RECOMMENDATIONS

#### (U//FOUO) FINDING ONE: Performance Standards, Performance Metrics, and Compliance Enforcement Measures for Targeting and Minimization Procedures Are Incomplete

(U//FOUO) Establishing accountability for compliance requires clear performance standards, measurement of actual performance against those standards, reporting results, and implementation of corrective action. These processes are not fully developed.

##### (U) Elements of an Effective Compliance Oversight Program

(S//NF) NSA has established a pre-tasking process that includes reviews of targeting requests for compliance with the targeting procedures. The targeting request must be approved before the selectors are released for tasking and collection. [REDACTED]

(b)(3)-P.L. 86-36

(U//FOUO) Effective compliance oversight requires the development of measurable standards against which actual performance can be assessed. Comparison of performance against these standards must be reported regularly to management for timely review and follow-up action. Together, these elements provide the means to establish accountability and initiate action to improve compliance.

##### (U) Shared Responsibility for Oversight

(S//NF) Monitoring compliance with FAA §702 targeting and minimization procedures has become a shared responsibility within the Agency. Before 2010, SID SV had primary responsibility for monitoring the Agency's application of FAA §702 authority. [REDACTED]

(b)(1)  
(b)(3)-P.L. 86-36

(S//NF) As personnel outside SV assumed more of the responsibility for adjudicating FAA §702 targeting requests, [REDACTED] trained new adjudicators [REDACTED]

(b)(3)-P.L. 86-36

~~TOP SECRET//SI//NOFORN~~

and assumed oversight of the targeting queue. Statistics on the targeting queue provide an assessment of the timeliness of the adjudication process and the means to evaluate the adequacy of the number of adjudicators given the volume of targeting requests [redacted]

(b)(1)  
(b)(3)-P.L. 86-36

[redacted] Although these

statistics inform management of the overall processing of targeting requests, they do not provide qualitative information regarding the accuracy of targeting requests submitted and approved and compliance with the targeting procedures.

(b)(3)-P.L. 86-36

(U//FOUO) SV's continuing oversight of analyst and adjudicator performance is effected through reviews of targeting requests (see Finding Three), participation in bi-monthly overseer reviews, and management of FAA §702 incident reporting. Errors identified in targeting requests are communicated to the analyst, adjudicator, and [redacted]. After overseer 60-day reviews, SV prepares feedback briefings to inform adjudicators of overseer findings. The briefings also provide metrics on the reasons for denial of targeting requests, trends identified in SW's review, and guidance on FAA §702 targeting procedures. Incident reports are also analyzed to identify trends that might require action. SV's oversight provides a critical assessment of compliance with FAA §702 independent of those requesting targeting. This feedback, however, is not provided to the managers responsible for the targeting analysts and adjudicators.

#### **(U) Development of FAA §702 Compliance Metrics**

(b)(3)-P.L. 86-36

(U//FOUO) S2 Compliance & FISA Staff [redacted] provides some metrics for FAA §702 processing and compliance, including weekly reports on the targeting request queue [redacted]

[redacted] The process to establish complete standards and measures for assessment of compliance continues.

(U//FOUO) To support effective monitoring of the Agency's use of FAA §702 authority, metrics must be:

- Based on clear and consistent expectations of performance for all targeting analysts and adjudicators within the Agency and

(b)(3)-P.L. 86-36

(U//FOUO)

~~TOP SECRET//SI//NOFORN~~

~~TOP SECRET//SI//NOFORN~~

- Generate sufficient detail to facilitate action by the adjudicator or targeting analyst.
- (b)(3)P.L. 86-36

(U) ~~FOUO~~ The development of these metrics by [ ] is not associated with the Comprehensive Mission Compliance Program, a group of NSA initiatives to achieve reasonable assurance that the SIGINT and Information Assurance missions are conducted in accordance with the laws and policies that protect USP privacy. The program includes monitoring and assessments, including trend analysis.

### **(U) Incomplete Implementation of Processes to Ensure Targeting Proficiency and Compliance Accountability**

---

(U) ~~FOUO~~ In 2010, SID completed the [ ] project, a Lean Six Sigma project to reduce targeting errors and improve processing efficiency and compliance for FAA transactions. The project team comprised personnel from [ ]

(b)(3)P.L. 86-36

[ ] Although several of the recommendations from [ ] have been implemented, recommendations that focused on accountability for targeting accuracy have not. The [ ] study recommended for FAA analysts:

- Employee performance review objectives for compliance with targeting requirements;
- Periodic metrics to leaders in organizations responsible for targeting (original focus was on denial metrics for FAA §702 targeting requests); and
- Progressive measures to improve compliance with targeting standards, including removal of FAA §702 targeting authority.

(b)(3)P.L. 86-36

(U) ~~FOUO~~ Although not addressed by the [ ] study, similar actions are needed to assess, monitor, and remediate the quality of targeting reviews conducted by adjudicators.

(U) ~~FOUO~~ To measure and increase targeting proficiency of the work force, including targeting under FAA §702 authority, SID [ ] has developed the Targeting Workforce Readiness Standard (WRS), Functional Job Qualification Standard (JQS) for all Agency personnel involved with targeting. Its purpose is to establish the standard targeting tasks along with the knowledge, skills, and abilities necessary to complete the tasks at a defined proficiency level.<sup>4</sup> The standard is supported by training and assessment plans (standard tests and on-the-job training evaluations). The WRS is under review and not fully implemented. Associated development

<sup>4</sup> (U) ~~FOUO~~ A functional JQS defines the standard of performance for a broad SIGINT function, such as targeting or reporting, and crosses skill communities, work roles, and personnel types. It applies to civilians (and contractors) as well as military personnel. The functional JQS, once completed at the specified proficiency level accompanies the individual across PLs and SID.

~~TOP SECRET//SI//NOFORN~~

~~TOP SECRET//SI//NOFORN~~

plans and a means to track progress are being created within the Associate Directorate for Education and Training's (ADET) Enterprise Learning Management (ELM) architecture and include much of the required training (classroom and on-the-job) for FAA §702 targeting analysts to achieve full proficiency. Implementation of the WRS and associated training and assessments will provide a means to achieve accountability for compliance with targeting requirements and ensure training standardization and enforcement. Development of FAA §702 metrics based on the WRS proficiency standards would support the performance measurement component of the WRS.

**(U//FOUO) RECOMMENDATION 1**

**(U//FOUO)** Establish for FAA §702 targeting analysts and adjudicators ACE performance objectives based on completion of a specified proficiency level of the Targeting Workforce Readiness Standard related ELM training plan.

**(S//NF) ACTION:** [REDACTED]**(U) Management Response**

(b)(3) P.L. 86-36

**(U//FOUO)** AGREE SID [REDACTED] are preparing an ELM plan for targeting analysts and adjudicators. The ELM plan will be broken down into proficiency levels, thereby allowing the analyst to register for the correct training as stated in the ACE objective. The ELM plan for the Targeting Workforce Readiness Standard for FAA §702 will be completed [REDACTED] ---, 1 for all National Cryptologic School (NCS) courses. Enforced registration in the ELM program and targeting proficiency statistics to the individual level as well as completion rate of any required FAA §702 training (NCS courses) will be completed [REDACTED]. Structured on-the-job training will be phased in.

**(U) Status:** OPEN**(U) Target Completion Date:** [REDACTED]

(b)(3) P.L. 86-36

**(U) OIG Comment****(U//FOUO)** Planned action satisfies the intent of the recommendation.~~TOP SECRET//SI//NOFORN~~

~~TOP SECRET//SI//NOFORN~~(U//~~FOUO~~) RECOMMENDATION 2

(U//~~FOUO~~) Develop metrics and management reporting to:

- (U//~~FOUO~~) Measure targeting analysis standardization to compliance with FAA §702 targeting and minimization procedures and
- (U//~~FOUO~~) Support analysis of trends indicative of changes needed in training or guidance.

(U//~~FOUO~~) Coordinate this process with the Comprehensive Mission Compliance Program.

(S//NF) ACTION: [REDACTED]

(b) (3)-P.L. 86-36

## (U) Management Response

(S//NF) AGREE [REDACTED] as part of the SID Lean Six Sigma Team. Participants will assess the feasibility of developing metrics to evaluate de-targeting trends and process deficiencies. Final implementation will depend on technical capabilities and deployment schedules.

(U) Status: OPEN

(U) Target Completion Date: [REDACTED] (b) (3)-P.L. 86-36

## (U) OIG Comment

(U//~~FOUO~~) Planned action satisfies the intent of the recommendation.

~~TOP SECRET//SI//NOFORN~~

(U) This page intentionally left blank.

~~TOP SECRET//SI//NOFORN~~

~~TOP SECRET//SI//NF//ORI~~~~(S//NF) FINDING TWO: Certain FAA §702 Selectors~~ [REDACTED]

(b)(1)  
(b)(3)-P.L. 86-36  
(b)(3)-50 USC 3024(i)

~~(TS//SI//NF)~~  
~~(TS//SI//NF//ORI)~~  
[REDACTED]~~(S//NF) Verification that Authorized Selectors Are on Collection~~~~(TS//SI//NF)~~  
[REDACTED]

(b)(1)f  
(b)(3)-P.L. 86-36  
(b)(3)-50 USC 3024(i)

~~(S//NF)~~  
[REDACTED]

~~(TS//SI//NF) The OIG's Report on the Assessment of Management Controls to Implement the Protect America Act (PAA) of 2007 (ST-08-00001), 7 April 2008.~~

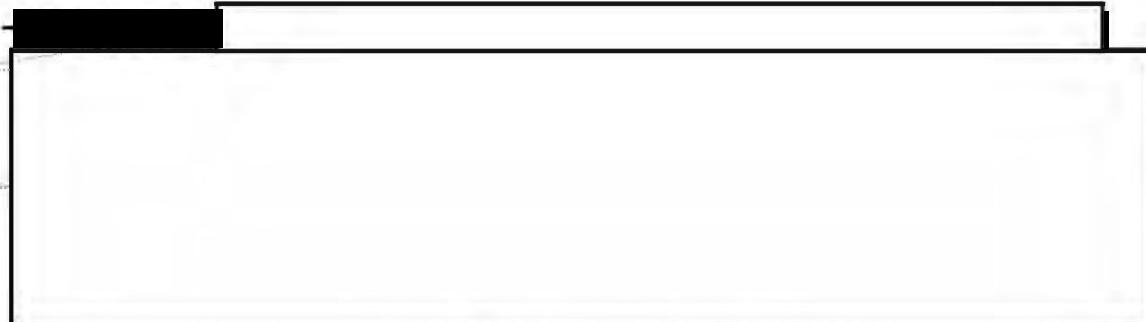
(b)(1)  
(b)(3)-P.L. 86-36  
(b)(3)-50 USC 3024(i)

~~(TS//SI//NF)~~  
[REDACTED]

(b)(1)  
(b)(3)-P.L. 86-36  
(b)(3)-50 USC 3024(i)

~~TOP SECRET//SI//NOFORN~~

(b)(1)  
(b)(3)-P.L. 86-36  
(b)(3)-50 USC 3024(i)

(U//~~FOUO~~) RECOMMENDATION 3

(TS//SI//NF)

(U//~~FOUO~~) ACTION:

(U) Management Response

(b)(3)-P.L. 86-36

(TS//SI//NF) AGREE

(b)(1)  
(b)(3)-P.L. 86-36  
(b)(3)-50 USC 3024(i)

(U) Status: OPEN

(U) Targett Completion Date: [REDACTED]

(b)(3)-P.L. 86-36

(U) OIG Comment

(U//~~FOUO~~) Planned action satisfies the intent of the recommendation.~~TOP SECRET//SI//NOFORN~~

~~TOP SECRET//SI//NF//ORN~~

**(U//FOUO) FINDING THREE: Oversight Requirements of FAA §702 Targeting Procedures and NSA Policy Are Not Fully Addressed**

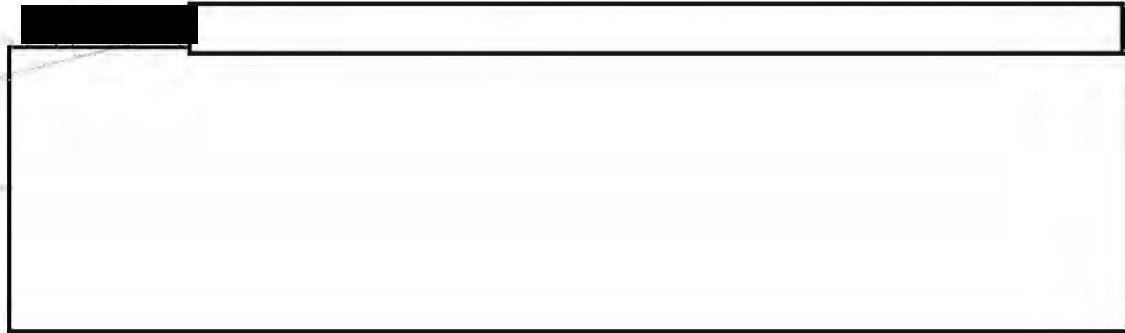
~~(TS//SI//NF)~~ SV oversight of FAA §702-sourced dissemination has not been modified to address requirements for multiple communication transactions. SV is implementing a new process for oversight of audits of FAA §702 database queries.

**(U//FOUO) Oversight of FAA §702 Dissemination**

~~(S//OFF)~~ The FAA §702 targeting procedures associated with the 2011 certifications require that SV perform "periodic spot checks...of intelligence disseminations to ensure compliance with established procedures...." SV performs spot checks of both serialized dissemination and dissemination of evaluated minimized traffic.

~~(TS//SI//NF)~~ FAA §702 minimization procedures establish unique requirements that analysts must implement. This includes the requirement that analysts document steps taken to verify that discrete communications within collection containing MCTs are eligible for dissemination. SV's spot-check of serialized dissemination does not include steps to verify that, when MCTs were used to support what is being disseminated, the MCT documentation required was prepared in accordance with the minimization procedures.

(b)(3)-P.L. 86-36



~~TOP SECRET//SI//NF//ORIN~~(U//~~FOUO~~) RECOMMENDATION 4

(TS//SI//NF) Although not required by the minimization procedures, SV should include in the spot-check of serialized disseminations of FAA §702-sourced material procedures to evaluate analysts' compliance with the documentation requirements pertaining to dissemination based on intelligence communications within MCTs. The spot-check should also evaluate proper use of [redacted] per NSA policy.

(b)(3)-P.L. 86-36

(U//~~FOUO~~) ACTION: SV

## (U) Management Response

(S//NF) AGREE [redacted] (b)(3)-P.L. 86-36  
[redacted] to modify the methodology and processes for spot-checking disseminations of FAA §702-sourced material.

(U) Status: OPEN

(U) Target Completion Date: [redacted]

## (U) OIG Comment

(U//~~FOUO~~) Closure of this recommendation will be evaluated upon receipt of documentation supporting the action taken.

(U) Oversight of Targeting Decisions

(S//NF) FAA §702 targeting procedures require that SV "conduct ongoing oversight activities and make any necessary reports, including those relating to incidents of noncompliance [with the FAA §702 targeting procedures]...and ensure that necessary corrective actions are taken to address any identified deficiencies." SV achieves oversight of targeting decisions through several means:

(b)(3)-P.L. 86-36

[redacted] SV's review includes analysis of the adequacy of the foreignness support for these targeting requests.

(b)(1)  
(b)(1)  
(b)(2)-P.L. 86-36  
(b)(3)-50 USC 3024(i)

selectors nominated by the CIA, [redacted]

(b)(3)-P.L. 86-36

~~TOP SECRET//SI//NF//ORIN~~

~~TOP SECRET//SI//NOFORN~~

implemented its own processes for nominating selectors. These are also adjudicated by SV.)

- SV reviews [REDACTED] self controls before (b)(3)-P.L. 86-36 sending them to the overseas bi-weekly [REDACTED]  
[REDACTED]
  - SV evaluates the targeting request for inconsistencies or inaccuracies and might review the sources cited to support foreignness if SV questions information [REDACTED]  
[REDACTED]
  - A full review, including sources supporting foreignness, is conducted for all targeting requests selected for review by DOJ/ODNI. Supporting documentation was reviewed for [REDACTED] of the (b)(3)-P.L. 86-36 targeting requests submitted for a recent review period.

~~(S//NF) Together, these processes give SV a perspective on the quality of the FAA §702 targeting and adjudication processes.~~

(U//~~FOUO~~) An assessment of compliance with the targeting procedures, based on SV's reviews of targeting requests, is not reported to management. Such reporting would aid in identification of trends, analyses and adjudicators whose performance demonstrates a need for additional training, and authoritative guidance in need of improvement.

~~(UNFOUO)~~ RECOMMENDATION 5

(U//FOUO) Periodically provide management reassessment of targeting analysis and adjudicator performance against the legal and policy requirements for FAA §702 targeting based on SV reviews of targeting requests. Coordinate with FAA §702 metrics reporting (see Recommendation 2).

(U//FOUO) ACTION: SV

## **(U) Management Response**

(U//~~FOUO~~) AGREE Per the requirements of Recommendation 2.j  
will incorporate metrics for management's assessment.

(U) Status: OPEN

(U) Target Completion Date: [REDACTED] (b)(3)-P L 86-36  
(b)(3)-P L 86-36

(U) OIG Comment

(U//~~FOUO~~) Planned action satisfies the intent of the recommendation.

~~TOP SECRET//SIAM//SIAM//NOFORN//~~

**(U) Oversight of FAA §702 Raw Traffic Repositories**

(U//~~FOUO~~) The FAA §702 targeting procedures for the 2011 certifications require that SV conduct periodic spot-checks of queries against repositories containing unevaluated and unminimized FAA §702 traffic. All queries of databases containing raw SIGINT content are subject to daily review by auditors assigned to each targeting analyst. Under U.S. Signals Intelligence Directive (USSID) CR 1610, Section A2.9, auditors must be trained in accordance with SV standards or meet with SV for a briefing on auditor responsibilities before conducting audits. USSID CR 1610 also requires that SV conduct "super audits" of all interactive raw SIGINT database systems.

(U//~~FOUO~~) Daily audits of queries assess compliance with FAA §702 query requirements. Oversight of the audits is necessary to ensure that they are properly and consistently executed. However, such reviews are not performed with regularity. SV has piloted and will soon fully implement a new super audit process that will examine the justifications for queries and evaluate query terms for foreignness using various Agency databases.

**(U//~~FOUO~~) RECOMMENDATION 6**

(U//~~FOUO~~) Implement the super audit process and provide periodic feedback to FAA §702 auditors and their management on the quality of audit performance.

(U//~~FOUO~~) ACTION: SV

**(U) Management Response**

(U//~~FOUO~~) AGREE SID/SV has fully implemented the super audit process for FAA 702. SID requests closure of the recommendation.

(U) Status: OPEN

**(U) OIG Comment**

(U//~~FOUO~~) Closure of this recommendation will be evaluated upon receipt of documentation supporting the action taken.

~~TOP SECRET//SI//NOFORN~~

**(U//FOUO) FINDING FOUR: Some Documentation Supporting Use of FAA §702 Authority Has Not Been Kept Up-to-Date and Requires Reorganization Across NSA Web Pages**

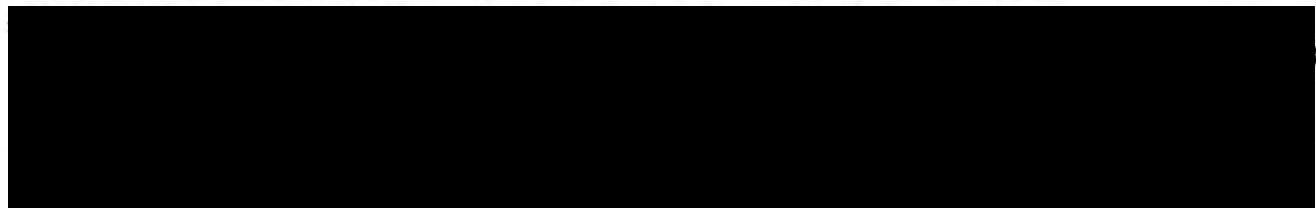
**(U//FOUO)** Guidance supporting compliant use of FAA §702 authority is maintained in several locations and is not fully organized by subject. Some of the guidance is outdated. Two Standard Operating Procedures (SOPs) provide differing guidance on the adjudication process. SOPs for some oversight functions have not been developed.

**(U) Maintenance of FAA §702 Guidance**

**(U//FOUO)** Part of the function of NSA's SOPs and other forms of guidance on FAA 702 is to instruct analysts and adjudicators in the proper use of FAA §702 authority. Included in the guidance are such topics as targeting, [redacted] dissemination, incident reporting, and the requirements for approval of FAA §702 targeting requests.

(b)(3)-P.L. 86-36

**(U//FOUO)** These instructions are found in several places, including the FAA, SV, and [redacted] web pages, the SV SharePoint site, and web pages maintained by individual S2 product lines. It is unclear whether some of the guidance is current because it refers only to PAA, the predecessor to FAA. In addition, much of the information on the FAA web page is presented as tips or appears in memorandum form, making it unclear whether it carries the same degree of authority as the SOPs.



**(U//FOUO)** The FAA web page, which should be the primary source of authoritative guidance, is owned by the [redacted]. [redacted] SID's FAA §702 Implementation Lead has been planning to update the guidance on this site, but other priorities, such as support for the 2011 FAA §702 Certification renewals, required attention.

(b)(3)-P.L. 86-36

**(U) Targetting Review: Two SOPs**

**(S//~~H~~OIF)** Two SOPs that provide guidance for adjudication of FAA requests have been issued [redacted] SV. [redacted] are the [redacted]

~~TOP SECRET//SI//NOFORN~~

Examples of [REDACTED] and common errors. It [REDACTED]

(b)(3)-P.L. 86-36 In contrast, the SOP published by [REDACTED] lists the roles and responsibilities for targeting analysts, releasers, and adjudicators reviewing FAA §702 targeting activities but does not provide a detailed description of the review requirements. Responsibility for training adjudicators now resides in [REDACTED] which should establish the authoritative guidance to support that training.

### **(U) SOPs for Oversight Activities**

(U) ~~FOUO~~ SOPs are key elements of a system of management controls. They establish performance expectations necessary to achieve corporate objectives, including compliance with established authorities.

(U) ~~FOUO~~ The Agency's use of FAA §702 authority is subject to monitoring by SV, S2 Mission Support Staff, and Agency personnel who oversee targeting analysts (including adjudicators). As noted already, guidance for targeting analysts and adjudicators has been developed by SV and S2 Mission Support Staff. It is important for the oversight functions to have documented procedures to ensure consistent execution of these functions despite staff turnover.

(S//NF) Responsibilities for FAA §702 oversight have changed significantly in the past year. SV performs reviews that support assessment of compliance with the authority by analysts and adjudicators, [REDACTED] [REDACTED] supports 60-day reviews of targeting and dissemination by DOJ/ODNI, and manages incident report investigation and follow-up. As personnel outside SV have accepted responsibility for review and approval of a significant portion of the targeting requests (including adjudicators across the Agency), the FAA Implementation Team has assumed responsibility for training and oversight of adjudicators and monitoring the targeting process. [REDACTED] has implemented the purge adjudication process to improve the completeness and accuracy of purges of FAA §702 data. SOPs for these oversight functions have not been fully developed.

(b)(3)-P.L. 86-36

### **(U) Role of the Rules Management Process**

(U) ~~FOUO~~ As part of NSA's Comprehensive Mission Compliance Program, the role of the ODOC [REDACTED] is to gather, organize, maintain and provide access to the information contained in external authorities, NSA/CSS policy, and compliance standards which govern NSA mission activities. The FAA §702 guidance should be maintained within this framework.

(b)(3)-P.L. 86-36

~~TOP SECRET//SI//NOFORN~~(U//~~FOUO~~) RECOMMENDATION 7

(U//~~FOUO~~) In accord with the Risk Management framework, establish a process to maintain authoritative guidance supporting compliant execution of FAA §702 authority:

- (U//~~FOUO~~) Organize this information to facilitate research by topic,
- (U//~~FOUO~~) Coordinate changes in guidance with required training, and
- (U//~~FOUO~~) Establish a single SOP as the guidance for adjudication of all FAA §702 targeting requests.

(b)(3)-P.L. 86-36

(U//~~FOUO~~) ACTION: [REDACTED]

## (U) Management Response

(U//~~FOUO~~) AGREE The following activities are in progress:

- [REDACTED] are developing and updating a single SOP for oversight, adjudication, and targeting FAA §702 functions and training.
- The [REDACTED] is populating FAA §702 documentation into a repository. In October 2012, SM/D worked with the [REDACTED] to discuss the process and progress.
- SV will collaborate with [REDACTED] to organize the "go FAA" and [REDACTED] FAA web pages.
- Guidance changes that require updates to NCS courses (within the CRSK series) will be requested via a New Learning Solution. In such case, [REDACTED] will be the originator upon coordination with SV. In addition, [REDACTED] (see Recommendation 1) will manage changes to the Targeting Workforce Readiness Standard and ELM training plan.

(U) Status: OPEN

(U) Target Completion Date: [REDACTED]

## (U) OIG Comment

(U//~~FOUO~~) Planned action satisfies the intent of the recommendation.

~~TOP SECRET//SI//NOFORN~~

~~TOP SECRET//SI//NOFORN~~

(U) This page intentionally left blank.

~~TOP SECRET//SI//NOFORN~~

**(U//FOUO) FINDING FIVE: Increased Automation of Processes Supporting FAA §702 Is Needed to Ensure Compliance and Reduce Errors**

~~(S/ASSISTANT)~~ the process for purge adjudication and execution relies on manual procedures that might result in incomplete and untimely processing. Eligibility for access to FAA §702 raw traffic databases is not verified after user accounts are established. Notices supporting required reviews [redacted] are not automated.

(b)(1)(i)

(b)(3)-P.L. 86-36

(b)(3)-50 USC 3024(i)

**(U) Purging of FAA §702 Records**

~~(U//FOUO)~~ The Agency identifies communications that must be removed from its systems by making a determination that content does not meet the standards for retention. Such records are ineligible as sources for Agency reports and must therefore be removed [redacted]. As these records are identified, they are added to the [redacted] or MPL. This system contains items that have been or are being evaluated for purge. NSA analysts rely on [redacted] as a primary source for reporting. To prevent improper use of purged records, all records sourced to a report are checked against the MPL, in real time, when a report is released. The [redacted] [redacted] are responsible for deleting records from their system based on an Execute Order, which is an authoritative request to remove data from the [redacted]. Completeness of the MPL as a register of records purged and full removal of records from the [redacted] are critical to compliance.

~~(U//FOUO)~~ FAA §702 records that analysts identify for purge are subject to adjudication by personnel in [redacted]. The review provides assurance that records subject to purge are completely identified. It also avoids purging records eligible for retention because they were collected under authorities in addition to FAA §702. [redacted] also coordinates [redacted] to execute the purge order.

~~(U//FOUO)~~ The adjudication process is manually intensive.

[redacted] personnel issue the execute order to the appropriate systems and conduct follow-up without automated support.

3<sup>rd</sup> error [redacted]

The manual process is subject to

[redacted] Lack of automation to complete the purge creates the opportunity for incomplete or untimely

~~TOP SECRET//SI//NF//OF//ORU~~

processing.

(b)(3)-P.L. 86-36

(U) ~~(FOUO)~~ No instances of inappropriate reporting were identified during this review which did not include testing.

**(U//FOUO) RECOMMENDATION 8**

~~(U//FOUO) Increase automation of the purge, adjudication, and execution processes to support complete and timely execution.~~

(U//FOUO) ACTION: [redacted]

**(U) Management Response**

(b)(3)-P.L. 86-36

(U) ~~(FOUO) AGREE~~ SID outlined a three phased approach to develop requirements for automation to improve purge processes efficiency, plan a schedule of work, and implement the new capabilities (see Appendix C for the detailed response).

(U) Status: OPEN

(U) Target Completion Date: [redacted]

**(U) OIG Comment**

(U) ~~(FOUO) Planned action satisfies the intent of the recommendation.~~

**(U//FOUO) Access Controls over FAA §702 Raw Traffic Databases**

(b)(3)-P.L. 86-36

~~(S//PRN) The FAA §702 targeting procedures associated with the 2011 certifications require that SV establish processes to ensure that raw traffic is accessible only to those who have had the proper training. Raw traffic derived from FAA §702 collection is maintained in [redacted]. To obtain a user account and access these databases, users must be assigned to an approved mission [redacted] obtain the~~

~~[redacted] access required for the database [redacted] and take required training. When all of these requirements have been met,~~

~~[redacted] an automated notice that permits establishment of an account. This process ensures that users have a mission need to access the information, understand the restrictions for handling the data, and have been properly trained in FAA §702 requirements.~~

(b)(3)-P.L. 86-36

(U//FOUO) [redacted] does not update training or access information after accounts have been established. [redacted] does not verify that persons accessing FAA §702 raw traffic databases continue to meet eligibility criteria. [redacted] can be used to verify this information; [redacted] began using

~~TOP SECRET//SI//NF//OF//ORU~~

~~TOP SECRET//SI//NOFORN~~

[redacted] for this purpose [redacted] Plans for [redacted] have not been established.

(U//FOUO) [redacted] provides authorization attributes and access control services to NSA enterprise programs and projects. NSA/CSSS Policy 6-311, Authentication and Authorization Services on NSANet Resources, 26 July 2010, requires that all legacy data repositories and applications be [redacted] enabled. According to the policy, a system is [redacted] enabled when it utilizes attributes about the user, obtained from [redacted] and applies authorization decisions based on those attributes." The Usage Guide states that, "authorization is based on privileges held such as security clearances, training completed [redacted] J [redacted]

(U//FOUO) Failure to verify user attributes that qualify for raw SIGINT access increases the risk of inappropriate access to FAA §702 raw traffic databases, although no such inappropriate access was identified by the OIG during this study.

#### (U//FOUO) RECOMMENDATION 9

(U//FOUO) Establish for repositories of FAA §702 data, [redacted] a means to verify that users remain eligible for access.

(b)(3)-P.L. 86-36 (U//FOUO) ACTION: [redacted]

#### (U) Management Response

(U//FOUO) AGREE [redacted] manages the mapping of access controls through [redacted] to repositories. Eligibility to access FAA §702 data is updated and reflected in [redacted] [redacted] are able to restrict access according to a user's eligibility status. This control was previously handled at a system level but is now managed by [redacted] SID requests closure of the recommendation.

(U) Status: OPEN

#### (U) OIG Comment

(U//FOUO) Closure of this recommendation will be evaluated upon receipt of documentation supporting the action taken.

#### ~~(S//NF)~~ [redacted] Required Reviews of FAA §702 Selections

b  
 (b)(1)  
 (b)(3)-P.L. 86-36 (b)(3)-50 USC 3024(i) (S//NF) Under FAA §702 authority, analysts are required, before tasking selectors, to determine that the intended target is a non-USPP reasonably believed to be outside the United States and confirm that the person is appropriate for targeting under FAA Certifications. After tasking is initiated and collection begins, the targeting procedures require NSA to conduct post-targeting analysis "designed to detect those occasions when a person who whom targeted was reasonably believed to be located outside the United

~~TOP SECRET//SI//NF//TQO~~

States has entered the United States, and will enable NSA to take steps to prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of acquisition to be located in the United States, or the intentional targeting of a person who is inside the United States."

~~(S//NF)~~ To ensure compliance with these requirements, the Agency has implemented the Obligation to Review (OTR) process, which establishes standards for post-tasking reviews. Initial target verification must be completed within five days of receipt of communications for the tasked selector. Analysts must confirm that:

- The user of the tasked selector is the intended foreign intelligence target,
- The target remains appropriate under the Certification cited in tasking and is not a USP, and
- The target remains outside the United States or there is no information to indicate that the target is inside the United States.

~~(S//NF)~~ After the initial verification, analysts must review sufficient information to verify that no change has occurred in the target's status that would affect eligibility for targeting. NSA's internal guidance directs that this review is to be done at least every 30 days. In addition to the requirements for review [redacted] analysts must determine whether the collection obtained is routinely of a type that might require prompt destruction (e.g., domestic communications).<sup>5</sup>

~~(S//SI//NF)~~ Automation has been implemented to support compliance with the OTR requirements. [redacted]



<sup>5</sup> ~~(U//FOUO)~~ Guidance to Analysts on Obligation to Review Data Under Protect America Act and the FISA Amendments Act (on the FAA web page).

~~TOP SECRET//SI//NOFORN~~

(b)(1)  
(b)(3)-P.L. 86-36  
(b)(3)-50 USC 3024(i)

**(U//FOUO) RECOMMENDATION 10**

(S//SI//NF) Improve accountability for compliance with NSA's internal OTR requirement:

- [REDACTED]
- [REDACTED]
- [REDACTED]

(b)(3)-P.L. 86-36

**(U//FOUO) ACTION:** [REDACTED]**(U) Management Response**

(S//SI//NF) AGREE SID reports that the requirements [REDACTED]

[REDACTED]  
are completed! [REDACTED]**(U) Status: OPEN****(U) Target Completion Date:** [REDACTED]

(b)(3)-P.L. 86-36

**(U) OIG Comment**

(U//FOUO) Planned action satisfies the intent of the recommendation.

~~TOP SECRET//SI//NOFORN~~

(U) This page intentionally left blank.

~~TOP SECRET//SI//NOFORN~~

**(U//FOUO) FINDING SIX: The FAA §702 Curriculum Needs to Be Updated and the Training Requirement Enforced**

(U//~~FOUO~~) Although the new FAA §702 course significantly improved training content, additional subjects should be considered, and the training should be enforced. An online resource supporting adjudicator training is needed.

#### (U) Analyst Training

(U) SID has significantly improved training for FAA §702

(U//~~FOUO~~) All personnel with access to FAA §702 raw traffic databases must take the training course "FISA Amendments Act (FAA) Section 702" (OWSC1203), which provides students with an understanding of the legal policies and minimization procedures for this authority.

(6)(F-P.L.C86:36)

**FAA §702 Practical Applications** is a [REDACTED] teachless application of FAA §702 authority. The course is part of the [REDACTED] which is establishing common standards and processes for SIGINT targeting and creating training and competency assessment mechanisms to support those standards. "FAA702 Practical Applications" will provide a tool to improve analyst understanding of how to apply FAA §702, including clear examples of documentation that meets the legal and policy requirements, and exercises in the use of the principles. Topics covered in the training include targeting requirements, selector research, documentation required to support the targeting decision, approval of targeting requests, analyst obligation to review communications to verify that selectors continue to meet targeting requirements, and incident research and reporting.

(U//FOUO) "FAA 702 Practical Applications" does not address certain topics important to compliance with FAA 702

~~(TS//SI//NF)~~ "FAA 702 Practical Applications" focuses on targeting and target maintenance. Certain matters were not included in the scope of the course, including handling of incidents resulting from improper minimization, dissemination, handling, and site tasking. Based on interviews with SID personnel and OIG review of the course, other matters should be considered for addition to the course.

- Explanation of the reasonable belief standard,
  - Reporting (including the new procedures required for handling MCTs),
  - Query requirements, and
  - Procedures for sharing FAA §702-derived information within the Agency and disseminating FAA §702-derived information to customers.

~~TOP SECRET//SI//NF//FORN~~

(U//~~FOUO~~) "FAA 702 Practical Applications" is not enforced for targeting under FAA §702 authority

(U//~~FOUO~~) According to S2 officials, completion of "FAA 702 Practical Applications" is required for analysts who have access to data derived from FAA §702 collection. The course offers more detailed training in the application of the authority and the potential to improve targeting efficiency and compliance with FAA §702. However, the requirement to take the course will not be enforced until ADET modifies the content to address deficiencies identified by [redacted] SID Operations personnel plan to begin enforcing the requirement for all analysts with access to FAA §702 information [redacted]

(b)(3)-P.L. 86-36

### **(U) Adjudicator Training**

(S//SI//NF) Adjudicators verify that targeting requests meet FAA §702 compliance standards before tasking. A significant training effort was undertaken [redacted]

(b)(3)-P.L. 86-36

[redacted] but a standardized online resource is needed to support current and future adjudicators. An online course would provide the basis for performance standards, support consistency of training, and serve as a ready reference when questions arise.

### **(U//~~FOUO~~) RECOMMENDATION 11**

(U//~~FOUO~~) Modify the FAA §702 curriculum:

- (U//~~FOUO~~) Include additional training on incidents (e.g., from improper minimization, dissemination) regarding requirements unique to FAA §702, query requirements, sharing of FAA §702-derived information, and explanation of the reasonable beliefs standard;
- (U//~~FOUO~~) Update "FAA 702 Practical Applications" and enforce the requirement for all FAA §702 analysts to complete the course; and
- (U//~~FOUO~~) Document the adjudicator training and make it available for reference.

(U//~~FOUO~~) ACTION: [redacted]

(b)(3)-P.L. 86-36

~~TOP SECRET//SI//NF//FORN~~

~~TOP SECRET//SI//NF//FOUO~~**(U) Management Response****(U) //FOUO) AGREE**

OVSC1203: SV will work with ADET to update the FAA §702 (OVSC1203) course to reflect the amended Targeting and Minimization Procedures that the Foreign Intelligence Surveillance Court approved in September 2012.

[REDACTED] will publish training slides onto the S2 FAA §702 Targeting Review Guidance web page and work with ADET to update OVSC1203D [REDACTED]

(b)(3)-P.L. 86-36  
CRSK 1304 & 1305: Updates to "FAA702 Practical Applications" (CRSK1304) and "FAA702 Adjudicator Training" (CRSK 1305) were completed [REDACTED]. In addition, enforced registration in the ELM program and targeting proficiency statistics to the individual level as well as completion rate of any required FAA §702 training (NCS courses) will be completed [REDACTED]. Structured on-the-job training will be phased in.

(U) Status: **OPEN**

(U) Target Completion Date: [REDACTED] ~1

**(U) OIG Comment**

(U) //FOUO) Planned action satisfies the intent of the recommendation.

**(U) Conclusion**

(U) //FOUO) NSA has designed a system of management controls, including training, policies, processes, procedures, systems, and oversight, to ensure compliance with FAA §702. Our recommendations suggest ways to improve the overall control environment in which the FAA §702 authority is used.

(U) This review examined the design of the controls. Compliance and substantive testing needed to draw conclusions on the efficacy of the management controls will be conducted in a later review.

~~TOP SECRET//SI//NF//FOUO~~

~~TOP SECRET//SI//NOFORN~~

(U) This page intentionally left blank.

~~TOP SECRET//SI//NOFORN~~

~~-TOP SECRET//SI//NOFORN-~~

## IV. (U) OBSERVATIONS

### **(U//FOUO) Procedures to Improve Representations to the FISC**

(U//FOUO) In an operation as diverse as NSA, where a multitude of legacy systems are involved in processing and compliance under a given authority, it is understandable that variations might exist in systems and manual procedures involved in the application of authority under FAA §702. These variations have the potential to create compliance concerns when standards are mandated for all users of an authority. [REDACTED] NSA expanded its universal Verification of Accuracy (VoA) procedures to NSA's FAA 702

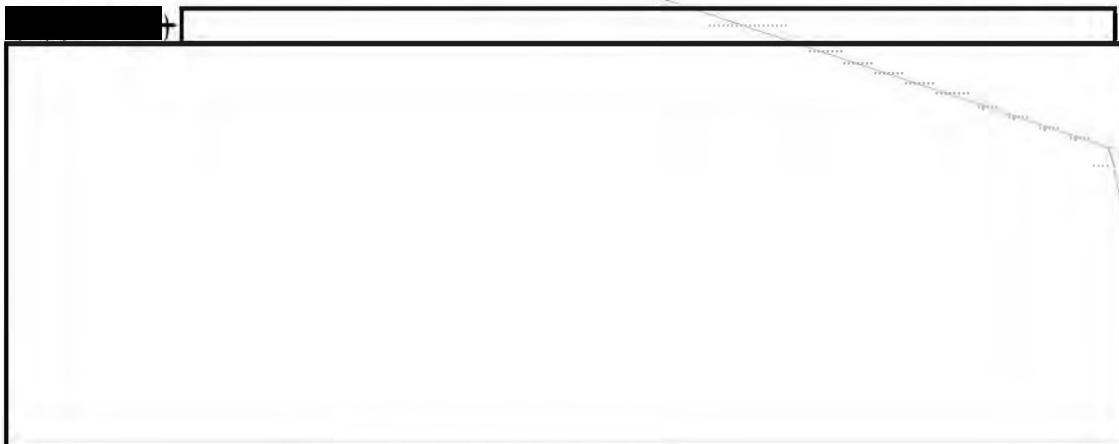
(b)(3)-P.L. 86-36

Minimization Procedures and Affidavits. NSA's VoA procedures are to be applied to written representations that describe NSA's acquisition, processing, retention, analysis, and dissemination and form the basis of a legal opinion, a FISC Order, or an Executive Branch decision or authority. The purpose of a VoA review is to increase confidence that the representations made to external entities are accurate and based on a shared understanding among operational, technical, legal, policy, and compliance officials. The VoA procedures require all factual statements within the declarations to be verified. Subject documents must be reviewed by authorizing individuals identified by senior leaders within the Directorates.

(U//FOUO) Additional training, maintenance of clear and updated guidance, and continued implementation of the VoA procedures will provide an increased level of confidence in obtaining a consistent understanding of Agency processes and in the accuracy of representations made regarding these processes to outside authorities (see Recommendations 7 and 11).

### **(U//FOUO) Effect of [REDACTED]**

### **(U//FOUO) Compliance with FAA §702**



(b)(3)-P.L. 86-36

~~-TOP SECRET//SI//NOFORN-~~

~~-TOP SECRET//SI//NF//ORI-~~**(U//FOUO) Effect of Manual Entry of Information on Targeting Requests**

-(S//NF) A significant requirement for processing targeting requests under FAA §702 authority is the documentation of support for analysts' determination that the target is outside the United States and is not a USP.

(b)(1)tr  
(b)(3)-P.L. 86-36  
(b)(3)-50 USC 3024(i)

-(S//NF) Before the targeting request is approved, adjudicators review the sources documented in the targeting request that support the foreignness of the selector.

(b)(1)  
(b)(3)-P.L. 86-36  
(b)(3)-50 USC 3024(i)

~~-TOP SECRET//SI//NF//ORI-~~

~~TOP SECRET//SI//NF//FOUO~~**V. (U//FOUO) SUMMARY OF RECOMMENDATIONS****(U//FOUO) RECOMMENDATION 1**

(U//FOUO) Establish for FAA §702 targeting analysts standard adjudication of CSEA performance objectives based on completion of a specified proficiency level of the Targeting Workforce Readiness Standard and [REDACTED] training plan.

(S//NF) ACTION: [REDACTED]

(U) Status: OPEN (b)(3)-P.L. 86-36

(U) Target Completion Date: [REDACTED]

**(U//FOUO) RECOMMENDATION 2**

(U//FOUO) Develop metrics and management reporting to:

- Measure targeting analysts and adjudicator compliance with FAA §702 targeting and minimization procedures and
- Support analysis of trends indicative of needed changes in training or guidance.

(U//FOUO) Coordinate this process with the Comprehensive Mission Compliance Program.

(S//NF) ACTION: [REDACTED]

(U) Status: OPEN (b)(3)-P.L. 86-36

(U) Target Completion Date: [REDACTED] (b)(1)

**(U//FOUO) RECOMMENDATION 3**

(b)(3)-P.L. 86-36

(b)(1)

(b)(3)-P.L. 86-36

(b)(3)-50 USC 3024(i)

(TS//SI//NF)

(U//FOUO) ACTION: [REDACTED] (b)(3)-P.L. 86-36

(U) Status: OPEN (b)(3)-P.L. 86-36

(U) Target Completion Date: [REDACTED]

**(U//FOUO) RECOMMENDATION 4**

(TS//SI//NF) Although not required by the minimization procedures, SV should include in the spot-check of disseminations of FAA §702-sourced material procedures to evaluate analysts' compliance with the documentation requirements pertaining to dissemination based on discrete communications within MCTs. The spot-check should also evaluate proper use of [REDACTED] per NSA policy.

(U//FOUO) ACTION: SV (b)(3)-P.L. 86-36

(U) Status: OPEN

(U) Target Completion Date: [REDACTED]

(U) OIG Comment: Closure of this recommendation will be evaluated upon receipt of documentation supporting the action taken.

~~TOP SECRET//SI//NF//FOUO~~

TOP SECRET//SI//NOFORN

## (U//FOUO) RECOMMENDATION 5

(U//FOUO) Periodically provide management an assessment of targeting analyst and adjudicator performance against the legal and policy requirements for FAA §702 targeting based on SV reviews of targeting requests. Coordinate with FAA §702 metrics reporting (see Recommendation 2).

## (U//FOUO) ACTION: SV

(U) Status: OPEN

(U) Target Completion Date: [REDACTED]

(b)(3)-P,L-86-36

## (U//FOUO) RECOMMENDATION 6

(U//FOUO) Implement the super audit process and provide periodic feedback to FAA §702 auditors and their management on the quality of audit performance.

## (U//FOUO) ACTION: SV

(U) Status: OPEN SID/SV reports the super audit process is fully implemented for FAA 702.

(U) OIG Comment: Closure of this recommendation will be evaluated upon receipt of documentation supporting the action taken.

## (U//FOUO) RECOMMENDATION 7

(U//FOUO) In conjunction with the Rules Management framework, establish a process to maintain authoritative guidance supporting compliant execution of FAA §702 authority:

- Organize the information to facilitate research by topic,
- Coordinate changes in guidance with required training and
- Establish a single SOP as the guidance for adjudication of all FAA §702 targeting requests.

## (U//FOUO) ACTION: [REDACTED] .....

(U) Status: OPEN

(U) Target Completion Date: [REDACTED]

## (U//FOUO) RECOMMENDATION 8

(U//FOUO) Increase automation of the purge adjudication and execution processes to support complete and timely execution.

## (U//FOUO) ACTION: [REDACTED] .....

(U) Status: OPEN

(U) Target Completion Date: [REDACTED]

(b)(3)-P,L-86-36

## (U//FOUO) RECOMMENDATION 9

(b)(3)-P,L-86-36

(U//FOUO) Establish for repositories of FAA §702 data, [REDACTED] a means to verify that users remain eligible for access.

## (U//FOUO) ACTION: [REDACTED] .....

(b)(3)-P,L-86-36

(U) Status: OPEN SID reports that actions have been taken to resolve the recommendation and requests its closure.

(U) OIG Comment: Closure of this recommendation will be evaluated upon receipt of documentation supporting the action taken.

~~TOP SECRET//SI//NOFORN~~(U//~~FOUO~~) RECOMMENDATION 10(U//~~FOUO~~) Improve accountability for compliance with NSA's internal DIRR requirement:

|   |  |    |
|---|--|----|
| 1 |  | // |
|---|--|----|

(U//~~FOUO~~) ACTION: [REDACTED], 1

(U) Status: OPEN

(U) Target Completion Date: [REDACTED] (b)(3)-P.L. 86-36

~~(b)(1)~~  
~~(b)(3)-P.L. 86-36~~  
~~(b)(3)-50 USC 3024(i)~~(U//~~FOUO~~) RECOMMENDATION 11(U//~~FOUO~~) Modify the FAA §702 curriculum:

- (U//~~FOUO~~) Include additional training on incidents (e.g., improper minimization, dissemination), reporting requirements unique to FAA §702, query requirements, sharing of FAA §702-derived information, and the application of the reasonable belief standard;
- (U//~~FOUO~~) Update "FAA702 Practical Applications" and enforce the requirement for all FAA §702 analysts to complete the course and
- (U//~~FOUO~~) Document the adjudicator training and make it available for reference.

(U//~~FOUO~~) ACTION: [REDACTED]

(U) Status: OPEN

(U) Target Completion Date: [REDACTED]

(b)(3)-P.L. 86-36

~~TOP SECRET//SI//NOFORN~~

~~TOP SECRET//SI//NOFORN~~

(U) This page intentionally left blank.

~~TOP SECRET//SI//NOFORN~~

~~TOP SECRET//SI//NOFORN~~**VI. (U) ABBREVIATIONS AND ORGANIZATIONS**

|                   |  |
|-------------------|--|
| (U) ADET          | Associate Directorate for Education and Training     |
| (U) CDW           | Corporate Data Warehouse                             |
| (S//NF) CIA       | Central Intelligence Agency                          |
| (U) DIRNSA        | Director of NSA                                      |
| (S//SI//NF) DNI   | Digital Network Intelligence                         |
| (S//SI//NF) DNR   | Dialed Number Recognition                            |
| (U) DOJ           | Department of Justice                                |
| (U) ELM           | Enterprise Learning Management                       |
| (U) FAA           | Foreign Intelligence Surveillance Act Amendments Act |
| (U) FBI           | Federal Bureau of Investigation                      |
| (U) FISA          | Foreign Intelligence Surveillance Act                |
| (U) FISC          | Foreign Intelligence Surveillance Court              |
| (U) ISP           | Internet Service Provider                            |
| (TBS//SI//NF) MCT | Multiple Communications Transactions                 |
| (U) MPL           | Master Purge List                                    |
| (U) NCS           | National Cryptologic School                          |
| (S//NF) NTOC      | NSA/CSS Threat Operations Center                     |
| (U) ODNI          | Office of the Director of National Intelligence      |
| (U) ODOC          | Office of the Director of Compliance                 |
| (U) OGC           | Office of General Counsel                            |
| (U) OIG           | Office of the Inspector General                      |
| (U) OTR           | Obligation to Review                                 |
| (U) PAA           | Protect America Act                                  |
| (U) PL            | Product Line   |
| (U)               |  |
| (U) S02           | SIGINT Policy and Corporate Issues Staff             |
| (U) S2~           | SID Analysis and Production                          |
| (U)               |  |
| (U)               |  |
| (b)(3)-P.L. 86-36 |  |
| (U)               |  |
| (U)               |  |
| (U) S3            | SID Directorate for Data Acquisition                 |
| (b)               |  |
| (U) SID           | Signals Intelligence Directorate                     |
| (U) SIGINT        | Signals Intelligence                                 |
| (U) SOP           | Standard Operating Procedure                         |
| (U)               |  |
| (U) SV            | SID Oversight and Compliance                         |
| (U) TD            | Technology Directorate                               |
| (U)               |  |
| (U)               |  |
| (U)               |  |
| (U) USP           | U.S. Person  |
| (U) USSID         | United States Signals Intelligence Directive         |

~~TOP SECRET//SI//NOFORN~~

~~TOP SECRET//SI//NOFORN~~

(U)   
(U) VoA

 Verification of Accuracy

(b)(3) P.L. 86-36

~~TOP SECRET//SI//NOFORN//  
100-000000000000000000~~

—TOP SECRET//SI//NOFORN—

**(U) APPENDIX A**

**(U) About the Study**

—TOP SECRET//SI//NOFORN—

~~TOP SECRET//SI//NOFORN~~

(U) This page intentionally left blank.

~~TOP SECRET//SI//NOFORN~~

## (U) ABOUT THE STUDY

### (U) Objectives

(U) ~~FOUO~~ The objective of this study was to assess the adequacy of management controls designed to provide reasonable assurance of compliance with Section 702 of the Foreign Intelligence Surveillance Act of 1978 (FISA), as amended by the FISA Amendments Act of 2008 (FAA §702).

### (U) Methodology

(U) ~~FOUO~~ This study was conducted from March 2011 to February 2012 and was based on review of published and draft forms of guidance; review of certain controls in systems supporting application of the authority; and interviews with managers and analysts responsible for targeting, approval, and oversight subject to FAA §702 requirements. (This report of the study's findings also incorporates information that was provided subsequently, primarily with respect to Finding Three.) Testing of the controls identified will be the subject of a later review.

(U) ~~FOUO~~ The study was conducted according to the standards of the *Council of the Inspectors General on Integrity and Efficiency Quality Standards for Inspection and Evaluation*, January 2011. We believe that the information derived from interviews and the documentation reviewed provides a reasonable basis for our findings, observations, and conclusions according to our study objectives.

### (U) Use of Computer-Processed Data

(U) The use of computer-processed data was not necessary to perform this audit.

### (U) Prior Coverage

(U) ~~FOUO~~ **Assessment of Management Controls to Implement the Protect America Act (PAA) of 2007**

(S//OF) The *Assessment of Management Controls to Implement the Protect America Act of 2007* found that additional controls were needed to verify that only authorized selectors were on collection and that tasked selectors were producing foreign intelligence on the expected targets. The study also identified the need for more rigorous controls to increase the reliability of spot checks for PAA compliance (PAA was the predecessor to FAA).

(U//FOUO) Audit of the FISA Amendments Act (FAA) §702 DeTasking Requirements

(S//PNF) the O/G Audit of the FISA Amendments Act (FAA) §702 DeTasking Requirements

and that the Agency does not have a consistent process to ensure a seamless transition from FAA §702 authority to FBI FISA.

(b) (1)  
(b) (3) -P.L. 86-36

~~TOP SECRET//SI//NOFORN~~

**(U) APPENDIX B**

**(U) FAA §702 Control Requirements  
and Management Controls**

~~TOP SECRET//SI//NOFORN~~

—TOP SECRET//SI//NOFORN—

ST-11-0009

(U) This page intentionally left blank.

—TOP SECRET//SI//NOFORN—

## (U) FAA §702 CONTROL REQUIREMENTS AND MANAGEMENT CONTROLS

(b) (1)  
(b) (3) -P.L. 86-36

(S//NF) Many of the internal control requirements are established by the Affidavit of the Director of NSA submitted for each Certification, Exhibit A to the Affidavit, and Exhibit 8 to the Affidavit.

[REDACTED]

Exhibit A sets forth the Agency's FAA §702 targeting procedures: the process for determining that a person targeted under Section 702 of the Foreign Intelligence Surveillance Act (FISA) Amendments Act of 2008 (FAA §702) authority is a non-U.S. person (NUP) reasonably believed to be located outside the United States; required post-targeting analysis to ensure that the Agency does not intentionally target a person known at the time of acquisition to be in the United States and does not result in intentional acquisition of domestic communications; required documentation of the foreignness determination; compliance and oversight; and steps required for departure from the procedures. Exhibit 8 contains the minimization procedures to be used for information collected. In addition to the control requirements established by the affidavits and exhibits, the Standards for Internal Control in the Federal Government provide a general framework of controls that should be incorporated into daily operations.

(U) This document provides a summary of the internal controls in place to meet these requirements.

ST-11-0009

|                          | Control Objective*  | Source        | Control Description  | Assessment |          |                   |
|--------------------------|---|---------------|--|------------|----------|-------------------|
|                          |   |               |  | Good       | Adequate | Needs Improvement |
| (U) TARGETING PROCEDURES |   |               |  |            |          |                   |
| 1                        | I. (U) Determination of Whether the Acquisition Targets Non-USPs Reasonably Believed to Be Located Outside the United States<br><br>TS//NF NSA determines whether a person is a non-USP reasonably believed to be outside the United States in light of the totality of the circumstances based on the information available with respect to the person. [REDACTED]<br><br>NSA analysts may use information from one or more of the following to make that determination:<br><br>Lead information<br>Research in NSA databases, available reports, and collateral information<br>[REDACTED] | (U) Exhibit A | <p>Targeting Requirements:</p> <p>[REDACTED]</p> <p>[REDACTED] the selector tasked and support for the reasonable belief of foreignness is also required.</p> <p>TS//NF The Targeting Rationale (TAR) Statement is also required and documents why targeting is requested and must indicate the tie to a foreign intelligence purpose specific to the FAA Certification under which targeting is requested.</p> <p>[REDACTED]</p> <p>TS//NF [REDACTED]<br/>[REDACTED] Releaser review, Signals Intelligence (SIGNIT) Directorate Product Line (PL) personnel review<br/>[REDACTED] Targeting Requests for overall compliance with the chosen FAA Certification before releasing it for adjudication</p> <p>TS//NF Adjudication: All targeting requests submitted under FAA §702 Certifications must pass this review for accuracy of processing and compliance with FAA §702 requirements. It includes the appropriateness of the target to the certification, verification of the support for reasonable belief of foreignness, confirmation that the most recent foreignness support is used, and that the information supports the non-USP status of the target. (See recommendation 11 regarding determination of a single Standard Operating Procedure (SOP) for adjudication.)</p> |            |          |                   |

(b)(1)  
 (b)(3)-P.L. 86-36  
 (b)(3)-50 USC 3024(i)

-TOP SECRET TS//NOFORN-  
 B-2

|   | Control Objective*  | Source        | Control Description   | Assessment |          |                   |
|---|---|---------------|---|------------|----------|-------------------|
|   |   |               |   | Good       | Adequate | Needs Improvement |
| 2 | (U) Determination of Whether the Acquisition Targets Non-USPs Reasonably Believed to Be Located Outside the United States (continued)   |               | <p>(U) Special Processing:<br/> <b>(S)(NF)</b> The Central Intelligence Agency (CIA) has its own nomination process. Requests are reviewed for FAA 5702 compliance by NSA personnel.</p> <p><b>(S)(NF)</b> FBI Tasking Requests: The FBI implemented its own nomination process subsequent to the field work on this study. <b>C-J</b></p> <p><b>(S)(CI/NF)</b></p> |            | H        | (b)(3)-P.L. 86-36 |
| 3 | (TS/SI/NF) To acquire communications about the target that are sent to or from the target, NSA will [redacted] to ensure that the person from whom it seeks to obtain foreign intelligence information is located overseas.<br><br><b>(S)(NF)</b> NSA will direct surveillance at a party to the communication reasonably believed to be outside the United States. | (U) Exhibit A | <p>(U) IP filters are used to ensure that one end of collected communications for DNI selectors is foreign (see special requirements for Multiple Communications Transactions (MCTs) – Minimization Procedures, row 4).</p> <p>(b)(1)<br/> (b)(3)-P.L. 86-36<br/> (b)(3)-50 USC 3024(i)</p>   |            | H        |                   |
| 4 | (U) Assessment of the Non-USP Status of the Target<br><br><b>(S)(NF)</b> Information that NSA examines to determine whether a target is reasonably believed to be located outside the United States might also bear on the non-USP status of the target. For example [redacted]   | (U) Exhibit A | (U) See Targeting Requirements (rows 1 and 2).  |            | H        |                   |

(b)(3)-P.L. 86-36

TOP SECRET//SI//NF//COMINT

B-3

ST-11-0009

~~TOP SECRET//SI//NF//FOUO~~(b)(1)  
(b)(3)-P.L.86-36  
(b)(3)-50 USC 3024(i)

|   | Control Objective*                                 | Source        | Control Description   | Assessment |          |                   |
|---|--|---------------|---|------------|----------|-------------------|
|   |  |               |   | Good       | Adequate | Needs Improvement |
| 5 | (S//NF) To prevent inadvertent targeting of a USP. | (U) Exhibit A | <p>(S//NF) [Redacted]</p> <p>(S//NF) [Redacted]</p> <p>(S//NF) If reasonable belief of foreignness is established [Redacted]</p> <p>The adjudicator's review verifies the reasonable belief of foreignness and that there is no contrary information concerning the target's LISP status.</p> <p>(b)(1)<br/>(b)(3)-P.L. 86-36</p> | #          |          |                   |

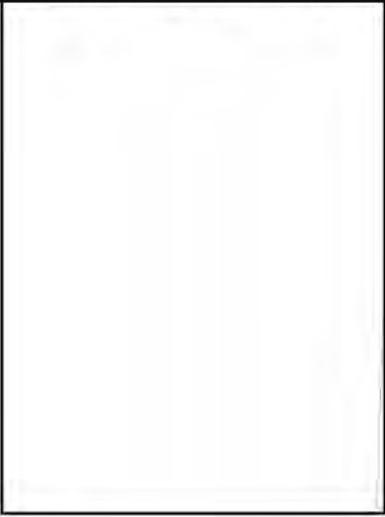
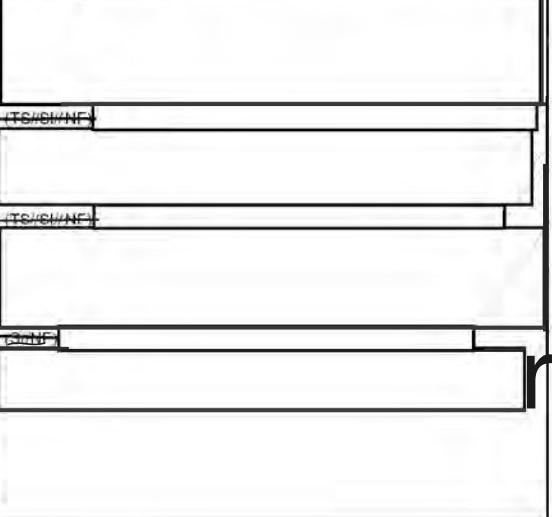
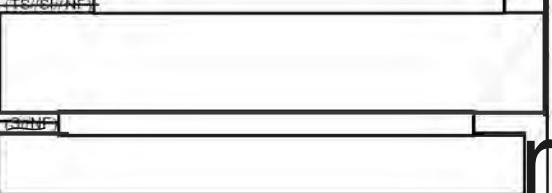
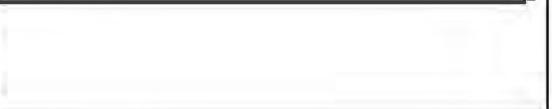
|   | Control Objective <sup>2</sup>  | Source        | Control Description  | Assessment |          |                   |
|---|---|---------------|--|------------|----------|-------------------|
|   |   |               |  | Good       | Adequate | Needs Improvement |
| 6 | (S//NF) Assessment of the Foreign Intelligence Purpose of the Targeting<br><br>[redacted] To assess whether the target possesses and/or is likely to communicate foreign intelligence information related to a foreign power [redacted]<br>[redacted] NSA considers information about selector including:<br>- [redacted]<br>- [redacted]<br>- [redacted] | (U) Exhibit A | (S//NF) The TAR Statement documents why targeting is requested and must indicate the tie to a foreign intelligence purpose specific to the FIMA Certification under which targeting is requested. This is subject to adjudication. | H          |          |                   |

(b)(1)  
(b)(3)-P.L. 86-36  
(b)(3)-50 USC 3024(i)

~~TOP SECRET//SI//NF//REL TO USA, UK, FVEY~~

B-5

ST-YL-0009

|   | Control Objective*  | Source        | Control Description   | Assessment |          |   |
|---|---|---------------|---|------------|----------|---|
|   |   |               |   | Good       | Adequate | Needs Improvement                                     |
| 7 | <p>II. (U//FOUO) POST -TARGETING ANALYSIS BY NSA</p> <p>(TS//SI//NF) Post-targeting analysis is designed to detect when a person who, when targeted, was reasonably believed to be located outside the United States has since entered the United States and will enable NSA to take steps to prevent intentional acquisition of communication from the sender and all intended recipients are known at the time of acquisition to be located in the United States, or the intentional targeting of a person who is in the United States. Such analysis may include:</p>  | (U) Exhibit A | <p>SP//NM NSA's Internal Obligation to Review (OTR) policy requires analysts to perform reviews as follows:</p> <ul style="list-style-type: none"> <li>- Initial collection must be reviewed within 5 days to verify that the user of the selector is the intended foreign intelligence target, the target is appropriate to the FAA Certification under which it is tasked, and the selector is not in the United States or a USP.</li> <li>- Collection must be reviewed at least every 30 days to affirm the target's foreignness and non-USP status and verify that information obtained is not of a type to require immediate destruction (e.g., domestic communications).</li> </ul> <p>(S//SI//NF)</p>  <p>(TS//SI//NF)</p>  <p>(TS//SI//NF)</p>  <p>(TS//SI//NF)</p>  |            |          | (b)(1)<br>(b)(3)-P.L. 86-36<br>(b)(3)-50 USC 3024(i)) |

(b)(1)  
(b)(3)-P.L. 86-36  
(b)(3)-50 USC 3024(i))

SECRET//NOFORN

|   | Control Objective*   | Source                                 | Control Description  | Assessment |          |                   |
|---|--|--|--|------------|----------|-------------------|
|   |  |  |  | Good       | Adequate | Needs Improvement |
| 8 | <p>III. (U) DOCUMENTATION</p> <p>(S//NF) Analysts who request tasking will document in the tasking database a citation or citations to the information that led them to reasonably believe that a targeted person is located outside the United States. Before tasking is approved, the database entry for that tasking will be reviewed to verify that the database entry contains the necessary citations.</p> <p>(S//NF) A citation is a reference that identifies the source of the information [redacted] which NSA will maintain. The citation will denote those responsible for conducting oversight to locate and review the information that led NSA analysts to conclude that a target is reasonably believed to be located outside the United States.</p> <p>(S//NF) Analysts also will identify the foreign power [redacted] about which they expect to obtain foreign intelligence.</p> | (U) Exhibit A<br><br>(b)(3)-P.L. 86-36 | <p>(S//NF) All targeting requests submitted under FAA §702 Certifications are subject to review by an adjudicator for verification of compliance with requirements including appropriateness of the target to the Certification, support for determination of foreignness and USP status, and foreign intelligence purpose. The adjudicator is responsible for ensuring that the support for reasonable belief of foreignness is documented in a database maintained by SID SV.</p> <p>(S//NF) The targeting system requires the analyst to choose from a menu of foreign intelligence purposes specific to each FAA §702 Certification. Once the certification is chosen, the analyst must select a [redacted] associated with that certification. If the [redacted] is not in the menu, the selector cannot be tasked under FAA authority.</p> <p>(b)(1)<br/>(b)(3)-P.L. 86-36<br/>(b)(3)-50 USC 3024(i)</p> |            | #        |                   |
| 9 | <p>IV. (U) OVERSIGHT AND COMPLIANCE</p> <p>(U//FOUO) SV with NSA's OGC will develop and deliver training to ensure that personnel responsible for approving targeting of persons under FAA §702, as well as analysts with access to the acquired foreign intelligence information, understand their responsibilities and the procedures that apply to this acquisition.</p>  | (U) Exhibit A                          | <p>(U//FOUO) Adjudicators are subject to the same training requirements as analysts. They also have received in-person training on the targeting review process. Documentation standardizing the information provided in this training has not been made available on-line for reference by the adjudicators.</p> <p>(U//FOUO) SV and OGC developed the "FISA Amendment Act (FAA) Section 702" course (DXSGC1208) when FPA was implemented. It focuses on the legal requirements of FAA.</p> <p>(U//FOUO) A new course, "FAA 702 Practical Applications" (CRSK1304), was made available [redacted]. It provides analysts with detailed examples of use of the authority. The requirement for its completion is not yet enforced (see Recommendation 11).</p>   |            | #        |                   |

(b) (3) - P.L. 86-36

-10-  
SECRET//SI//NOFORN  
B-7

ST-11-0009

|    | Control Objective*   | Source                                 | Control Description   | Assessment |          |   |
|----|--|--|---|------------|----------|---|
|    |  |  |   | Good       | Adequate | Needs Improvement                                   |
| 10 | (U//FOUO) SV has established processes for ensuring that raw traffic is labeled and stored only in authorized repositories and is accessible only to those who have had the proper training. | (U) Exhibit A<br><br>(b)(3)-P.L. 86-36 | <p>(U//FOUO) All collection stores must be compliance certified before they can be used to process or store FAA §702 data.</p> <p>(U//FOUO) All FAA §702 systems are certified for purge and access functions.</p> <p>(U//FOUO) To obtain access to the FAA §702 databases, individuals must have an approved mission (entered in [redacted] by their supervisor), appropriate clearances (supervisor must request in the [redacted] System), and required training (Overview of Intelligence Authorities, USSID 101 Legal Compliance and Minimization Procedures, and OVSC1203).</p> <p>(B)(1)(NF) Requests for analysts' access do [redacted]<br/>[redacted] containing FAA §702 data [redacted] be submitted by a mission sponsor [redacted] access must be approved by the [redacted] owner.</p> <p>(U//FOUO) SV reviews requests for compartmented accesses, verifying that the analyst has required training and an appropriate justification for access (e.g., includes mission function, targets requiring FAA access).</p> <p>(U//FOUO) [redacted] are not able to verify an account holder's continuing eligibility to access FAA §702-derived collection. Eligibility is determined when the account is established. Compliance with annual requirements of appropriate training is not verified at sign-on after account sign-up (this was corrected for [redacted] in a system update [redacted] (see Recommendation 9).</p> |            |          | (b)(1)<br>(b)(3)-P.L. 86-36<br>(b)(3)-S USG 3024(i) |

(b)(3)-P.L. 86-36

|    | Control Objective <sup>2</sup>   | Source        | Control Description  | Assessment |          |  |
|----|--|---------------|--|------------|----------|--|
|    |  |               |  | Good       | Adequate | Needs Improvement                                    |
| 11 | (U//FOUO) SV will conduct oversight activities and will make necessary reports, including those relating to incidents of non-compliance, to the NSA Inspector General and OGC. SV will also ensure that corrective actions are taken to address identified deficiencies. To that end, SV will conduct periodic spot checks of targeting decisions and intelligence disseminations to ensure compliance with established procedures and conduct periodic spot checks of queries in data repositories. | (U) Exhibit A | <p>(U) Incident Reporting – see row 13.</p> <p>(U//FOUO) SV performs the following oversight activities:</p> <ul style="list-style-type: none"> <li>- [redacted] newly tasked or reassigned before sending to DOJ and Office of the Director of National Intelligence (ODNI) bi-weekly.</li> <li>- Review targeting support for the bulk of items requested by DOJ/ODNI for the 60-day review. If support is insufficient, SV will follow up with the adjudicator and targeting analyst for additional support or corrective action (including possible detasking).</li> <li>- Spot check serialized reports based on FAA §702 information, reports containing USP identifiers, and evaluated, minimized traffic [redacted] C:1. Follow-up on identified discrepancies. Provide record of all FAA §702-derived dissemination for review by DOJ/ODNI and follow up on any issues identified during their review. SV's spot check of serialized disseminations does not include procedures [redacted].</li> <li>- Verification of analysis compliance with the minimization procedures' documentation requirements for dissemination derived from MCITs (see Recommendation 4).</li> <li>- Oversight of Queries: All queries are reviewed daily by auditors in the SLD production centers. SV has not conducted reviews of auditor performance consistently (see Recommendation 6).</li> </ul> |            |          | (b)(1)<br>(b)(3)-P.L. 86-36<br>(b)(3)-50 USC 3024(i) |
| 12 | (U//FOUO) DOJ and ODNI will conduct oversight of NSA's exercise of (FAA §702 authority), which will include periodic reviews by DOJ and ODNI personnel to evaluate the implementation of the procedures. Such reviews will occur at least once every 60 days.  | (U) Exhibit A | <p>(U//FOUO) SV coordinates bi-monthly reviews by DOJ/ODNI of targeting and dissemination, including responding to questions raised and providing feedback sessions to adjudicators on the overseers' findings.</p> <p>(U//FOUO) DOJ performs reviews every 60 days covering all tasks and dissemination for a two-month period. Every 15 days, SV sends a document to DOJ for each certification, one each for DNI and DNR listing all the key fields for the review.</p> <p>[redacted]</p> <p>DOJ sends NSA a spreadsheet of the selectors chosen for review. SV must gather all supporting material for each selector.</p>  |            |          | (b)(3)-P.L. 86-                                      |

~~TOP SECRET//NOFORN~~

B-9

ST-II-0009

|    | Control Objective*   | Source        | Control Description  | Assessment |          |  |
|----|--|---------------|--|------------|----------|--|
|    |  |               |  | Good       | Adequate | Needs Improvement                          |
| 13 | <p>(U//FOUO) NSA will report to DOJ and ODNI incidents of non-compliance with these procedures by NSA personnel that result in the intentional targeting of a person reasonably believed to be located in the United States, the intentional targeting of a USP, or the intentional acquisition of communication in which the sender and all intended recipients are known at the time of acquisition to be located within the United States.</p> <p>(U//FOUO) NSA will provide such reports within 5 business days of learning of the incident.</p> <p>(U//FOUO) Information acquired by intentionally targeting a USP or a person not reasonably believed to be outside the United States at the time of such targeting will be purged from NSA databases.</p> | (U) Exhibit A | <p>(U) Incident Research/Reporting:</p> <p>(U//FOUO) SV and the targeting team research potential incidents jointly. SV maintains records of the incidents [redacted] in a SharePoint database. SV manages the follow-up process to produce the required notice to DOJ/ODNI within 5 business days of confirmation of an incident.</p> <p>(U//FOUO) [redacted]</p> <p>(U//FOUO) [redacted]</p> <p>(U//FOUO) [redacted]</p> <p>(S//NF) OGC reviews the incident and ultimately determines whether it meets the criteria for reporting to DOJ/ODNI. For incidents of non-compliance with procedures (e.g., failure to appropriately task a selector, over-collection), NSA must explain why it happened and what steps were taken to remediate the matter (e.g., purge data, provide additional training). DOJ determines whether the matter must be reported to the FISC in accordance with Rule 13(b) of the FISC Rules of Procedure.</p> <p>(U//FOUO) The Target of Primary Interest ((TOP)) provides SV with the parameters for necessary purge of collection. SV enters this in the incident record in SharePoint. S2's [redacted]</p> <p>[redacted] uses this information to initiate the purge process, verifying that the parameters include all affected collection methods containing information eligible for retention. I [redacted]</p> <p>The purge process relies on manual procedures that create a risk of incomplete or untimely purge execution (see Recommendation 8).</p> |            |          | (b)(3)-P.L. 86-36<br>(b)(3)-50 USC 3024(i) |

(b)(3)-P.L. 86-36

B-10

~~TOP SECRET//SI//M//P//R//N~~

|    | Control Objective <sup>2</sup>   | Source                                 | Central Description   | Assessment |          |  |
|----|--|--|---|------------|----------|--|
|    |  |  |   | Good       | Adequate | Needs Improvement                                    |
| 14 | (S//NF) NSA will report to DOJ and ODNI incidents of non-compliance (including over-collection) by any electronic communication service provider to whom the Attorney General and Director of National Intelligence issued a directive under §702. Such report will be made within 5 business days after determining that the provider has not complied or does not intend to comply with a directive.   | (U) Exhibit A                          | (S//NF//SI//M//P//R//N) Per OGC, the same incident reporting process is used for matters involving providers [redacted] incident reports [redacted] as a result of provider error have been filed with the FISC.<br>[redacted]<br>[redacted]  |            |          | (b)(1)<br>(b)(3)-P.L. 86-36                          |
| 15 | (S//NF) In the event that NSA concludes that a person is reasonably believed to be located outside the United States and after targeting, learns that the person is inside the United States or if NSA concludes that a person, who at the time of targeting, was believed to be a non-USP was in fact a USP, it will take the following steps:<br><br>1. Terminate the acquisition without delay. If NSA inadvertently acquires a communication sent to or from the target while the target was located inside the United States, including communication in which the sender and all intended recipients are reasonably believed to be located inside the United States at the time of acquisition, such communication will be treated in accordance with the minimization procedures.<br>2. Report the incident to DOJ and ODNI within 5 business days. | (U) Exhibit A<br><br>(b)(3)-P.L. 86-36 | (S//NF//SI//M//P//R//N) It is the analyst's responsibility to follow up on [redacted] information from review of traffic and detask all related selectors promptly if the target is in the United States or identified as a USP. The primary user is not the target [redacted]<br>[redacted] An incident is initiated [redacted]<br>[redacted] Identification of roaming or a change in USP status through review of collection [redacted]<br>[redacted] The targeting team works with SV to document the incident. Information captured in the Incident Report database includes the detasking date, whether other selectors associated with the target were detasked, and parameters for purge of communications collected that are ineligible for retention. SV follows up with PL personnel to ensure that the incident record is complete, including entry of purge criteria.<br>(S//NF) [redacted] selector management ensures that [redacted] incident follow-up are handled timely, regardless of analyst turnover or absence. [redacted] is responsible for timely follow-up.<br>Note: Implementation of [redacted] will add controls over the process, including a requirement for PL management to document their review that the incident record is complete.<br>[redacted]<br>[redacted]<br>(U) See Row 13 – Incident Reporting. |            |          | (b)(1)<br>(b)(3)-P.L. 86-36<br>(b)(3)-50 USC 3024(i) |

~~TOP SECRET//SI//M//P//R//N~~

ST-11-0009

|                                    | Control Objective*  | Source                   | Control Description   | Assessment         |          |  |
|------------------------------------|---|--------------------------|---|--------------------|----------|--|
|                                    |   |                          |   | Good               | Adequate | Needs Improvement                                |
| 16                                 | V. (U) DEPARTURE FROM PROCEDURES<br><br>TS//NF If, to protect against an immediate threat to national security, NSA determines that it must take action temporarily in apparent departure from these procedures and it is not feasible to obtain a timely modification of these procedures from the Attorney General and Director of National Intelligence, NSA may take such action and will report that activity promptly to DOJ. Under such circumstances, NSA will continue to adhere to all of the statutory limitations set forth in the Act. | (U) Exhibit A            | (U//FOUO) According to OGC, such actions would be coordinated by that department and involve personnel at the highest levels of the Agency; DOJ/ODNI would be notified. No specific procedures or controls have been developed.   |                    | #        |  |
| <b>(U) MINIMIZATION PROCEDURES</b> |   |                          |   |                    |          |  |
| 1                                  | III. (U) Acquisition and Processing -General<br><br>(a) TS//SI//NF Acquisition of information by targeting non-USPs reasonably believed to be located outside the United States pursuant to FAA §702 will be effected in accordance with an authorization made by the Attorney General and Director of National Intelligence and will be conducted in a manner designed, to the greatest extent possible, to minimize the acquisition of information not relevant to the authorized purpose of the acquisition.                                     | (U) Exhibit B, Section 3 | (U//FOUO) See targeting and adjudication processes: foreignness criteria, TAR, etc. (rows 1 through 6 of Targeting Procedures).<br><br>(TS//SI//NF) [REDACTED]<br><br>(U//FOUO) manages over-collection events. [REDACTED] they may stop collection.<br><br>(U//NF) FAA §702 query procedures define specific requirements for use of [REDACTED] in query selection terms.<br><br>(U//NF) Daily audits of queries [REDACTED] identify overly broad queries (excessive targeting). | (b) (3)-P.L. 86-36 | #        | (b)(1)<br>(b)(3)-P.L. 86-36<br>(b)(3)-50 USC 302 |

~~TOP SECRET//SI//NF//IN~~

|   | Control Objective <sup>a</sup>   | Source   | Control Description   | Assessment   |          |                   |
|---|--|--|---|--|----------|-------------------|
|   |  |  |   | Good   | Adequate | Needs Improvement |
| 2 | <p>(b) (U) Monitoring, Recording, and Processing<br/>           (1) (G)(S)(H)(F) Personnel will exercise reasonable judgment in determining whether information acquired must be minimized and will destroy inadvertently acquired communications or concerning a USP at the earliest practicable point in the processing cycle at which such communication can be identified either as clearly not relevant to the authorized purpose of the acquisition (e.g., the communication does not contain foreign intelligence information) or as not containing evidence of a crime that may be disseminated under these procedures.</p> <p>(R)(G)(H)(F) Except for Internet transaction from upstream collection, inadvertently acquired communications or concerning a USP may be retained no longer than 5 years from the expiration date of the certification authorizing the collection.</p> | (U) Exhibit BB, Section 3<br><br>(b)(3)-P.L. 86-36 | <p>(U//FOUO) The FAA §702 training course (OVSC1203) specifies the steps analysts are to take to analyze communications for eligibility for retention.</p> <p>[REDACTED]</p> <p>[REDACTED] provides direction for retention/destruction on the basis of whether the target was outside the United States at the time of collection and whether the communication is foreign or domestic.</p> <p>(R)(H)(F) Unless an incident is reported from improper acquisition of such communications, there is no review process to ensure that analysts identify and destroy them as required. The cost of such control would be prohibitive. The requirement is that all identified issues of improper collection be reported to SV and an Incident Initiated. Performance standards and analysis of actual versus expected performance could improve accountability for compliance (see Recommendations 1-4).</p> <p>(U) Examination of retention controls was not included in this review.</p>   | (b)(1)<br>(b)(3)-P.L. 86-36<br>(b)(3)-50 USC 3024(i) |          |                   |
| 3 | <p>(4) (G)(S)(H)(F) As a communication is reviewed, analysts will determine whether it is a domestic or foreign communication to, from, or about a target and is reasonably believed to contain foreign intelligence information or evidence of a crime. Only such communications may be processed. All other communications may be retained or disseminated only in accordance with procedures</p> <p>[REDACTED]</p>  | (U) Exhibit BB, Section 3<br><br>(b)(3)-P.L. 86-36 | <p>(U//SI//NF) [REDACTED] provides direction for retention/destruction on the basis of whether the target was outside the United States at the time of collection and whether the communication is foreign or domestic. This is covered in detail in OVSC1203, the required FAA §702 training.</p> <p>(U) See also Obligation to Review – row 7 of Targeting Procedures.</p> <p>(U//FOUO) Parameters for purge of collection associated with an incident are provided to SV by the TOPI and recorded in the incident record in SharePoint. S2 Purge and Pretasking Compliance uses this to initiate the purge process, verifying that all affected data is identified. Without running, information is held for retention.</p> <p>[REDACTED]</p> <p>[REDACTED] SV performs follow-up to verify that Purge and Pretasking Compliance has updated the incident record with the status of purge completion. The purge process relies on manual procedures that create a risk of incomplete or untimely purge execution (see Recommendation 8).</p> <p>(R)(G)(H)(F) SV works with TOPIs to prepare destruction waivers for objects that meet purge criteria and contains significant foreign intelligence value or evidence of a crime or threat of harm. The Destruction Waiver must be approved by DDIRNSA.</p> |  |          |                   |

~~TOP SECRET//SI//NF//IN~~

ST-11-0009

|   | Control Objective*   | Source                   | Control Description   | Assessment |          |                   |
|---|--|--------------------------|---|------------|----------|-------------------|
|   |  |                          |   | Good       | Adequate | Needs Improvement |
| 4 | <p>III. (b)(5) (TS/G/NF) Processing of Internet Transactions Acquired through NSA Upstream Collection Techniques</p> <p>(a) (TS/G/NF) NSA will take reasonable steps after acquisition to identify and segregate through technical means Internet transactions that cannot be reasonably identified as containing single, discrete communications in which the active user of the transaction (i.e., the selector used to send or receive the Internet transaction to or from a service provider) is reasonably believed to be located in the United States.</p> <p>(b) (TS/G/NF) Such segregated communications will be retained in an access-controlled repository accessible only to NSA analysts trained to review such transactions for the purpose of identifying those that contain discrete communications in which the sender and all intended recipients are reasonably believed to be located in the United States.</p> | (U) Exhibit B, Section 3 | <p>(TS/G/NF) The Technology Directorate developed procedures to analyze upstream collection. Data permitted for use by analysts must have the active user (sender or recipient) be the target or be outside the United States (currently approximately [redacted] of upstream collection). Data is sequestered when the active user is reasonably believed to be in the United States [redacted]</p> <p>[redacted]</p> <p>(TS/G/NF) There is no training on use of MCTs at this time (see Recommendation 11).</p> <p>(b)(1)</p> <p>(b)(3)-P.L. 86-36</p> <p>(b)(3)-50 USC 3024(i)</p> <p>(U/PDO) Efforts are ongoing to develop processes for removing data from sequestration and special training for analysts who will process this data (no recommendation - in process).</p> |            |          | H                 |
| 5 | <p>III. (b)(5)b. (TS/G/NF) NSA analysts seeking to use a discrete communication within an Internet transaction that contains multiple discrete communications will assess whether the discrete communication (1) is a communication in which the sender and all intended recipients are located in the United States and (2) is to, from, or about a tasked selector or otherwise contains foreign intelligence information.</p> <p>III. (b)(5)b.3. (TS/G/NF)</p> <p>[redacted]</p>  | (U) Exhibit B, Section 3 | <p>(TS/G/NF) Procedures are documented for use of upstream collection</p> <p>[redacted]</p> <p>Training on application of these procedures has not been developed (see Recommendation 11).</p> <p>(b)(1)</p> <p>(b)(3)-P.L. 86-36</p> <p>(b)(3)-50 USC 3024(i)</p>  |            |          | H                 |

TOP SECRET//SI//NF//FORN  
B-14

~~TOP SECRET//SI//COMINT~~

|   | Control Objective*  | Source  | Central Description   | Assessment |          |                   |
|---|---|---|---|------------|----------|-------------------|
|   |   |   |   | Good       | Adequate | Needs Improvement |
| 6 | <p>III. (b)(6) TSP/SHINF Magnetic tapes or other storage media containing FAA §702-derived communications may be queried to identify and select communications for analysis. Query terms used will be limited to selection terms reasonably likely to return foreign intelligence information. Identifiers of an identifiable USP may not be used as terms to identify and select for analysis any Internet communication acquired through NSA's upstream collection techniques.</p> <p>(S/SHINF) Any use of USP identifiers as terms to identify and select communications must first be approved in accordance with NSA procedures. NSA will maintain records of all USP identifiers approved for use as selection terms.</p> | (U) Exhibit B, Section 3<br><br><b>(b)(1)</b><br><b>(b)(3)-P.L. 86-36</b><br><b>(b)(3)-50 USC 3024(i)</b> | <p>(S/SHINF) Guidance on queries of FAA Databases states that NSA may not use USP names or identifiers as selection terms When reviewing collected FAA §702 data.</p> <p>(U/FOLIO) Queries are subject to review by auditors in the B2 production centers to verify that the query has a foreign intelligence purpose within mission scope and reasonably excludes protected data.</p> <p>(U/FOLIO) Reviews of the audits performed by PL personnel have not been regularly executed by SV to ensure quality of the audit process (see Recommendation 6).</p> <p style="text-align: center;"><b>(b)(3)-P.L. 86-36</b></p>   |            |          | a                 |
| 7 | <p>III. (c) (U/FOLIO) Destruction of Raw Data</p> <p>TSP/SHINF Communications acquired under FAA §702 authorities other than through upstream collection that do not meet the collectors standards set forth in these procedures and that are known to contain communications of or concerning USPs will be destroyed upon recognition and may be retained no longer than 5 years from the expiration date of the certification authorizing the collection.</p>   | (U) Exhibit B, Section 3<br><br><b>(b)(1)</b><br><b>(b)(3)-P.L. 86-36</b><br><b>(b)(3)-50 USC 3024(i)</b> | <p>(S/SHINF) [redacted] provides direction for retention/destruction on the basis of whether the target was outside the United States at the time of collection and whether the communication is foreign or domestic. This is also covered in detail in OVSC1203, the required FAA §702 training.</p> <p>(U) See also Obligation to Review - row 7 of Targeting Procedures.</p> <p>(S/SHINF) A matrix of scenarios/reasons purge action is required is documented for authorities including FAA §702. Purges are identified as part of the incident investigation process. SV and the TOPI capture the purge parameters in the incident record on the SV SharePoint site. The purge adjudication team performs research to verify completeness of items identified for purge.</p> <p>[redacted] (U) Purge adjudication and execution is manual and subject to error affecting completeness and timeliness (see Recommendation 8).</p> <p>(U/FOLIO) Purge Process: [redacted]</p> <p>[redacted] are responsible for deleting records from their system on the basis of a Purge Execute Order, to prevent improper use of purge records to support reporting.</p> <p>(S/SHINF) [redacted]</p> <p>(U) Retention - outside scope.</p> |            |          | a                 |

~~TOP SECRET//MM//NP//SI~~

ST-YL-0009

|   | Control Objective*   | Source                   | Control Description<br>(b)(3)-P.L. 86-36  | Assessment |          |  |
|---|--|--------------------------|---|------------|----------|--|
|   |  |                          |   | Good       | Adequate | Needs Improvement                                    |
| 8 | <p>(TS//SI//NF) Internet transactions that are acquired through NSA's upstream collection and do not contain information that meets the retention standards set forth in these procedures and that are known to contain communication of or concerning USPs will be destroyed upon recognition. All upstream collection may be retained no longer than 2 years from the expiration date of the certification authorizing the collection. The Internet transactions that may be retained include those that were acquired because of limitations on NSA's ability to filter communications.</p>   | (U) Exhibit B, Section 3 | <p>(U) See also Obligation to Review -row 7 of Targeting Procedures.</p> <p>(S//SI//NF) [redacted] provides direction for retention/destruction on the basis of whether the target was outside the United States at the time of collection and whether the communication is foreign or domestic. This is also covered in detail in OVSC1203, the required FAA §702 training.</p> <p>(U) (a) The need to purge communications is identified as part of the incident investigation process; SV and the TOPI capture the purge parameters in the incident record on the SV SharePoint site. The purge adjudication team performs research to verify completeness of items identified for purge. Purge adjudication and execution is manual and subject to error affecting completeness and timeliness (see Recommendation 8).</p> <p>(U) Retention -outside scope.</p> |            |          | H  |
| 9 | <p>III.(d) (U) Change in Target's Location or Status</p> <p>(S//SI//NF) In the event that NSA determines that a person reasonably believed to be located outside the United States and, after targeting the person, learns that the person is inside the United States or if NSA concludes that a person who, at the time of targeting, was believed to be a non-USP is in fact a USP, the acquisition from that person will be terminated without delay.</p> <p>(S//SI//NF) Communications acquired through the targeting of a person who at the time of targeting was reasonably believed to be located outside the United States but was in fact located inside the United States at the time such communications were acquired, and any communications acquired by targeting a person who at the time of targeting was believed to be a non-USP but was in fact a USP, will be treated as domestic communications.</p> | (U) Exhibit B, Section 3 | <p>(U) See also Obligation to Review -row 7 of Targeting Procedures.</p> <p>(S//SI//NF) Detasking guidance states that analysts are responsible for detasking a selector upon review of content indicating that the selector is used by a USP, confirmation that the selector is being used by an individual in the United States. [redacted]</p> <p>[redacted]</p> <p>(U) See row 7 for purge procedures.</p>  |            |          | (b)(1)<br>(b)(3)-P.L. 86-36<br>(b)(3)-50 USC 3024(i) |

~~TOP SECRET//SI//NOFORN~~

B-16

~~TOP SECRET//SI//NF//FORA~~

|    | Control Objective*  | Source                   | Control Description   | Assessment |          |                   |
|----|---|--------------------------|---|------------|----------|-------------------|
|    |   |                          |   | Good       | Adequate | Needs Improvement |
| 10 | IV.(U) OGC Acquisition and Processing – Attorney-Client Communications<br><br><del>(S//SI//NF)</del> As soon as it becomes apparent that a communication is between a person who is known to be under criminal indictment in the United States and an attorney who represents that individual in the matter, monitoring of that communication will cease and the communication will be identified as an attorney-client communication in a log maintained for that purpose. The relevant portion of the communication containing that conversation will be segregated, and the National Security Division of DOJ will be notified. In addition, all proposed disseminations of information constituting USP attorney-client privileged communications must be reviewed by OGC before dissemination. | (U) Exhibit B, Section 4 | <del>(S//SI//NF)</del> OGC reports that no instances of such collection have been identified to date by NSA analysts, and therefore, no log has been initiated. Such instances would be rare (e.g., it would occur only if a person reasonably believed to be outside the United States is targeted by NSA known to be under indictment in the United States and NSA intercepts a communication between the target and an attorney representing that foreign person in the U.S. legal proceeding).              |            | N/A      |                   |
| 11 | V. (U) Domestic Communications<br><br><del>(TS//SI//NF)</del> A communication identified as a domestic communication will be promptly destroyed upon recognition unless DIRNSA (or Acting DIRNSA) specifically determines, in writing, that it meets certain criteria (e.g., contains significant foreign intelligence, evidence of a crime).<br><br><del>(S//SI//NF)</del> If a domestic communication indicates that a target has entered the United States, NSA may advise the FBI of that fact.   | (U) Exhibit B, Section 5 | <del>(TS//SI//NF)</del> Communication that is determined to be domestic (does not have at least one communicant outside the United States) will be promptly destroyed upon recognition unless DIRNSA specifically determines in writing that the communication may be retained. SV works with TCOPIs to prepare destruction waivers. This process is monitored as part of the follow-up on incidents and purges.  |            | H        |                   |
| 12 | VI. (U) Foreign Communications of or Concerning USPs<br><br>(a) (U) Retention<br><br><del>(S//SI//NF)</del> Foreign communications of or concerning USPs may be retained only if necessary for the maintenance of technical databases, if dissemination of such communications with reference to such USPs would be permitted under subsection (b), or if the information is evidence of a crime and is provided to appropriate federal law enforcement authorities.  | (U) Exhibit B, Section 6 | <del>(TS//SI//NF)</del> Communication resulting from the targeting of a person who was reasonably believed at the time of targeting to be a non-USP located overseas but is later determined to be a USP or a person in the United States will be promptly destroyed upon recognition unless DIRNSA specifically determines in writing that the communication may be retained. SV works with TCOPIs to prepare destruction waivers. This process is monitored as part of the follow-up on incidents and purges. |            | H        |                   |

~~TOP SECRET//SI//NF//FORA~~

|    | Control Objective*  | Source                   | Control Description   | Assessment |          |                   |
|----|---|--------------------------|---|------------|----------|-------------------|
|    |   |                          |   | Good       | Adequate | Needs Improvement |
| 13 | VI. (b) (U) Dissemination<br><del>(S//NF)</del> A report based on communications of or concerning a USP may be disseminated in accordance with Section VII or VIII if the identity of the USP is masked. Otherwise, dissemination of intelligence reports based on communications of or concerning a USP may be made only to a recipient requiring the identity of such person for the performance of official duties that meet certain criteria. | (U) Exhibit B, Section 6 | (U//FOUO) This restriction on dissemination is not unique to FAA §702 and is consistent with procedures required by Executive Order (E.O.) 12333.<br><br><b>(b)(1)<br/>(b)(3)-P.L. 86-36</b>  |            | #        |                   |
| 14 | VI. (c) <del>(S//NF)</del> Provision of Unminimized Communications to CIA and FBI<br><del>(S//NF)</del> NSA may provide to the CIA and FBI unminimized communications derived from FAA §702 collection.   | (U) Exhibit B, Section 6 | (TS//SI//NF)<br><br><del>(S//NF)</del> Discussion of FAA §702 collection with CIA/FBI: If IC analysts have their own copy of the data, provided through CIA nomination or FBI dual route, NSA analysts may discuss the information with them. They may not provide copies of the information to IC personnel. This is addressed in required NSA/CSS Policy 11-1, Information Sharing.   |            | #        |                   |
| 15 | VII. (U) Other Foreign Communications<br><br>(U) Foreign communications of or concerning a non-USP may be retained, used, and disseminated in any form in accordance with other applicable law, regulation, and policy.   | (U) Exhibit B, Section 7 | (U//FOUO) Dissemination is handled in accordance with the Foreign Intelligence Surveillance Act Amendments Act of 2008, the Minimization Procedures Used by the National Security Agency in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended, DoD Regulation 5240.1-R Procedures Governing the Activities of DOD Intelligence Components That Affect United States Persons and the Classified Annex to Department of Defense Procedures Under Executive Order 12333. |            | #        |                   |

~~TOP SECRET//SI//NF//PORN~~

B-18

|                         | Control Objective*   | Source                   | Control Description   | Assessment |          |  |
|-------------------------|--|--------------------------|---|------------|----------|--|
|                         |  |                          |   | Good       | Adequate | Needs Improvement                          |
| 16                      | <p>VIII. (S//NF) Collaboration with Foreign Governments</p> <p>(a) (S//NF) Procedures for the dissemination of evaluated and minimized information: Information acquired under FAA §702 may be disseminated to a foreign government. Other than in cases for linguistic assistance by a foreign government (Section VIII (b)), dissemination to a foreign government of information of or concerning a USP may be done only in a manner consistent with subsections VI (b) and VII (rows 13 and 15).</p> <p>(b) (S//NF) Procedures for technical or linguistic assistance: Communications that, because of their technical or linguistic content, may require further analysis by foreign governments to assist NSA in determining their meaning or significance. NSA may disseminate items containing unminimized FAA §702 information to foreign governments for analysis, under certain restrictions.</p> | (U) Exhibit B, Section 8 | <p>(S//NF) Sharing Evaluated and Minimized</p> <p>(S//NF) Evaluated and minimized</p> <p>(S//NF)</p> <p>(S//NF)</p> <p>(S//NF)</p> <p>(S//NF) The provision for technical/linguistic assistance</p> <p>Documentation is developed case by case. Consideration should be given to documentation of this process.</p> |            |          | (b)(3)-P.L. 86-36<br>(b)(3)-50 USC 3024(i) |
| (U) MANAGEMENT CONTROLS |  |                          |   |            |          |  |

|   | Control Objective*  | Source   | Control Description  | Assessment |          |   |
|---|---|--|--|------------|----------|---|
|   |   |  |  | Good       | Adequate | Needs Improvement                               |
| 1 | (U) Activities must be established to monitor performance measures and indicators. Controls should be aimed at validating the propriety and integrity of organizational and individual performance measures and indicators.   | (U) Standards for Internal Control in the Federal Government | (U//FOUO) Annual performance objectives for compliance with FAA §702 requirements, associated policy, and SOPs have not been established (see Recommendation 1).   |            |          | H   |
| 2 | (U) Information should be recorded and communicated to management and others within the entity who need it and in a form and within a time frame that enables them to carry out their internal control and other responsibilities.  | (U) Standards for Internal Control in the Federal Government | (U//FOUO) Comparison of actual performance to established standards for compliance activities associated with FAA §702 are incomplete (see Recommendations 2, 4, 5, and 6).  |            |          | H   |
| 3 | (U) Internal control monitoring should assess the quality of performance over time and ensure that findings are resolved. It includes regular management and supervisory activities, such as ongoing comparisons and reconciliations, to ensure that controls are functioning properly. | (U) Standards for Internal Control in the Federal Government | (U//FOUO) [REDACTED]   |            |          | (b)(1)<br>(b)(3)-P,L; 86-36<br>(b)(3)-50 LSC 30 |
| 4 | (U) Access to resources and records should be limited to authorized individuals.  | (U) Standards for Internal Control in the Federal Government | (U//FOUO) To share FAA §702 information with other NASA analysts, steps must be taken to ensure that the individual has the proper clearance. This information is not addressed in the required FAA §702 training and guidance is not available on the FAA web page (see Recommendation 11). |            |          | H   |

~~TOP SECRET//SI//NF//INFORN~~

B-20

~~TOP SECRET//SI//NOFORN~~

**(U) APPENDIX C**

**(U) Full Text of Management Response**

~~TOP SECRET//SI//NOFORN~~

~~TOP SECRET//SI//NOFORN~~

ST-11-0009

(U) This page intentionally left blank

~~TOP SECRET//SI//NOFORN~~

[REDACTED]

**SIGNALS INTELLIGENCE  
DIRECTORATE  
memorandum**

22 February 2013

FROM: Signals Intelligence Directorate (SID)

TO: Office of the Inspector General (OIG); ATTN: [REDACTED]

(b) (3) - P.L. 86-36

SUBJ: (U//FOUO) SID Response to the Revised Report on the OIG Assessment of Management Controls Over FAA 702 (ST-11-0009).

(U) The purpose of this memorandum is to provide SID's revised response to the subject report which includes updates to corrective action plans, content adjustments, and technical minutiae to ensure accuracy.

(U//FOUO) SID reviewed the revised report in its entirety. The attached response acknowledges SID's agreement with eleven recommendations and provides revised corrective action plans, points of contact, and target completion dates as needed.

M-11-10M The SID consolidated response is attached to this memorandum. Please call S022-966-5621(s) if you have any questions.

[REDACTED] (b) (3) - P.L. 86-36

[REDACTED]

Deputy Chief of Staff for  
SIGINT Policy and Corporate Issues (S02)

Encl: a/s

~~TOP SECRET//SI//FOUO//RPN~~

ST-11-0009

~~TOP SECRET//SI//FOUO//RPN~~**NSA/CSS OFFICE OF INSPECTOR GENERAL**

**(U) OFFICE OF INSPECTOR GENERAL (OIG) DRAFT REPORT:**  
**Assessment of Management Controls Over FAA §702**

**Management Response to Draft Report**

(U) In accordance with IG-11357-12, "Coordinating Office of Inspector General Reports," the purpose of the draft coordination phase is to gain management's agreement or disagreement with report findings and recommendations. The SIGINT Directorate (SID) has been extended an opportunity to review and comment on the revised report to ensure contextual accuracy.

(U) The following matrix includes SID's consolidated revisions to management's action plans where applicable.

| Rec. No. | Action                             | Agree or Disagree | Management Response  | Completion date                 |
|----------|------------------------------------|-------------------|--|---------------------------------|
| 1        | SMNFI SID<br>[REDACTED]<br>with SV | Agree             | <p>(U//FOUO) [REDACTED] agrees with the recommendation. The [REDACTED] and [REDACTED] are currently preparing an ELM plan for Target Analysts and Adjudicators. This plan will include FAA 702-specific training.</p> <p>(U) POC: [REDACTED] f"<br/> (U//FOUO) [REDACTED] 963-0561</p> <p><u>Revised Management Response:</u><br/> (U//FOUO) [REDACTED] are preparing an ELM plan for target analysts and adjudicators. The ELM plan will be broken down into proficiency levels thus allowing the analysts to register for the correct training based on proficiency level as stated in the ACE objective. The ELM plan for the Targeting workforce readiness standard for FAA §702 will be completely [REDACTED] for all NCS courses. Enforced registration in the ELM program and targeting proficiency statistics to the individual level as well as completion rate of any required FAA §702 training (NCS courses) will be completed [REDACTED]. Structured OJT training will be phased in</p> | (b)(3)-P.L.866366<br>[REDACTED] |

Derived From: NSA/CSSM 1-52

Dated: 20070108

Declassify On: 20376601

~~TOP SECRET//SI//FOUO//RPN~~

[REDACTED]

~~TOP SECRET//SI//NOFORN~~

ST-11-0009

|   |                     |       |   |            |
|---|---------------------|-------|---|------------|
|   |                     |       | <u>Revised Target Completion Date:</u><br>[redacted]  |            |
|   |                     |       | <u>Revised POC:</u><br><del>(U//FOUO)</del> [redacted]<br>969-6728  |            |
| 2 | (U//NF) SID with SV | Agree | (S//NF) [redacted] will work with [redacted] as part of the SID Lean Six Sigma Team. Participants will assess the feasibility of developing metrics to evaluate de-targeting trends and process deficiencies. Final implementation will be dependent on technical capabilities and deployment schedules.<br><br>(U) POC:<br><del>(U//FOUO)</del> [redacted] 963-0561<br><br><u>Revised POC:</u><br><del>(U//FOUO)</del> [redacted] 969-6729 | [redacted] |
| 3 | (U//NF) OGC         | Agree | (TS//SI//NF) [redacted] k16<br><br>Oversight & Compliance (SV), [redacted]<br><br>(S//NF) Will convene to establish technical procedures to implement a reconciliation process.<br><br>(U) POC:<br><del>(U//FOUO)</del> [redacted] 769-2449<br><br><u>Revised Target Completion Date:</u><br>[redacted]   | [redacted] |
| 4 | (U) SV with OGC     | Agree | (S//NF) SID/SV will collaborate with [redacted] and OGC to establish a methodology and process for spot-checking dissemination of AA702-sourced material dependent on the volume of dissemination.<br><br>(U) POC:<br><del>(U//FOUO)</del> [redacted] 966-2479  | [redacted] |

(b)(1)  
 (b)(3)P.L. 86366  
 (b)(3)50 USC 302

~~TOP SECRET//SI//NOFORN~~

~~TOP SECRET//SI//FOUO//IN~~

ST-11-0009

ST-11-0009

|   |  |       |   |                    |
|---|--|-------|---|--------------------|
|   |  |       | <b>Revised Management Response:</b><br><del>(U//FOUO) SID/SV will collaborate with [REDACTED]</del><br><br>[REDACTED] and OGC to modify the methodology and process for spot-checking dissemination of FAA §702-sourced material.   |                    |
|   |  |       | <b>Revised Target Completion Date:</b><br>[REDACTED]  |                    |
| 5 | (U)SV                                      | Agree | (U//FOUO) Per the requirements of Recommendation 2, SID/SV will incorporate metrics for management's assessment.<br><br>(U) POC:<br>(U//FOUO) [REDACTED] SV6966-2479  | (b) (3)-P.L. 86-36 |
| 6 | (U)SV                                      | Agree | (U//FOUO) SID/SV has fully implemented the super audit process for FAA 702. SID requests closure of the subject recommendation.<br><br>(U) POC:<br>(U//FOUO) [REDACTED] SV6966-2479   | Request Closure    |
| 7 | (U)SID [REDACTED] SV, [REDACTED] with ODOC | Agree | (S//NF) The following activities are currently in progress:<br><br><ul style="list-style-type: none"> <li>- SID/SV [REDACTED] are developing and updating a single SOP for oversight, adjudication and targeting FAA 702 functions and training.</li> <li>• [REDACTED] is currently populating FAA 702 documentation into a repository. [REDACTED] Inc. SID [REDACTED] will work with the [REDACTED] to discuss the process and progress.</li> <li>• SV will collaborate with S2 and [REDACTED] to organize the "go FAA" and "dt:JFAA" web pages.</li> </ul><br>(U) POC:<br>(U//FOUO) [REDACTED] 966-5597<br><br><b>Revised Management Response:</b><br><del>(U//FOUO) Add bullet #4: Guidance changes that require updates to NCS courses (within the CRSK series) will be</del> |                    |

~~TOP SECRET//SI//FOUO//IN~~

~~TOP SECRET//SI//NOFORN~~

ST-11-0009

|   |                    |       |  |  |
|---|--------------------|-------|--|--|
|   |                    |       | <p><b>(b)(3)-P.L. 86-36</b></p> <p>requested via a New Learning Solution. In such case [redacted] will be the originator upon coordination with SV. In addition, [redacted] (see recommendation 1) will manage changes to flagging Workforce Readiness Standard add ELM training plan.</p> <p><b>Revised Target Completion Date:</b><br/>[redacted]</p> <p><b>Revised RODC:</b><br/><b>(U//FOUO)</b> [redacted]<br/>963-1109</p>   |  |
| 8 | (U) SDR [redacted] | Agree | <p><b>(U//FOUO) Phase 1: Requirements Gathering:</b></p> <ul style="list-style-type: none"> <li>• Conduct technical exchanges sessions with [redacted] developers.</li> <li>• Direct participation of the [redacted] including detailed briefings of the purge process and requirements.</li> <li>• Document recommendations for specific areas where automation will improve process efficiency.</li> <li>• Update the compliance steering group on automation requirements and existing gaps.</li> </ul> <p><b>(U//FOUO) Phase 1 Deliverable:</b><br/>Report documenting reviews and technical exchanges with [redacted]. This will include an implementation plan.</p> <p><b>(U) Target Completion:</b><br/>[redacted]</p> <p><b>(U//FOUO) Phase 2: Planning Phase:</b><br/>Per the development and implementation plan, create a schedule of work required to increase automation of the purge adjudication and execution processes.</p> <p><b>(U//FOUO) Phase 2 Deliverable:</b><br/>Coordinate with [redacted] to document a schedule/timeline with specific completion tasks required to enhance this capability per the implementation plan.</p> |  |

~~TOP SECRET//SI//NOFORN~~~~TOP SECRET//SI//NOFORN~~

ST-III-0009

TOP SECRET//SI//FOUO//NOFORN

ST-11-0009

|   |                           |       |   |                 |
|---|---------------------------|-------|---|-----------------|
|   |                           |       | (U// <del>FOUO</del> ) Phase 3:<br>Development/Implementation:<br>Work with [redacted] to develop the new<br>capability per Phase 1 and 2.<br><br>(U// <del>FOUO</del> ) Phase 3 Deliverable:<br>Complete the development and provide<br>a final report to OIG defining results.<br><br>(U) POC:<br>(U// <del>FOUO</del> ) [redacted]<br>963-0561 |                 |
|   |                           |       | (b)(3)-PL. 1<br><br>(U) POC:<br>(U// <del>FOUO</del> ) [redacted]<br>963-0561<br><br>Revised Management Response:<br>(U// <del>FOUO</del> ) SID [redacted] manages the<br>mapping of access controls through<br>[redacted] to repositories.<br><br>Eligibility to access FAA §702 data is   | Request Closure |
| 9 | (U) STS - J<br>[redacted] | Agree | (U// <del>FOUO</del> ) SID requests closure of the<br>recommendations. Deliverable<br>Update: The SID Data Manager can<br>provide documentation to enable<br>closure of this recommendation.  |                 |

TOP SECRET//SI//FOUO//NOFORN

TOP SECRET//SI//FOUO//NOFORN

ST-11-0009

|    |                               |       |   |  |
|----|-------------------------------|-------|---|--|
|    |                               |       | <b>Revised POC:</b><br>(U//FOUO) [REDACTED]<br>969-6729 & [REDACTED]<br>[REDACTED] 963-3004   |  |
|    |                               |       | <b>(U) Sub-bullet #1:</b><br>(S//NF) Per DNI OTR guidelines, the requirements of sub-bullet #1 are completed.<br>[REDACTED]<br>[REDACTED]<br>The analyst must assess traffic and respond to three supporting questions.<br>[REDACTED]   |  |
| 10 | (U//SI) [REDACTED]            | Agree | <b>(U) Sub-bullet #2:</b><br>(S//SI//NF) The [REDACTED] organizations are currently developing<br>[REDACTED]<br><br><b>(U) POC:</b><br>(U//FOUO) [REDACTED] 969-6729<br><br><b>Revised POC:</b><br>(U//FOUO) [REDACTED] 969-6729  |  |
| 11 | (U//SI)<br>[REDACTED]<br>ADET |       | <b>(U//SI//NF) Sub-bullet 1 &amp; 2:</b><br>SID [REDACTED] referred to SV. SV will work with ADET to update the following course: FISA Amendment Act (FAAA) Section 702 (OVSC1203) to reflect modified Targeting and Minimization Procedures that are currently pending the Foreign Intelligence Surveillance Court ruling.<br><br><b>(U//SI//NF) Sub-bullet 3:</b> SID [REDACTED] will publish training slides onto the S2 FAA 702 Targeting Review Guidance webpage and will work with ADET to develop a course to replace briefings and informal training sessions.<br><br><b>(U) POC:</b><br>(U//FOUO) [REDACTED] |  |

TOP SECRET//SI//NF//NOFORN

TOP SECRET//SI//NF//NOFORN

(b)(1)  
(b)(3)-P.L.863-36  
(b)(3)-50 USC 302

~~-TOP SECRET//SI//U//FORN~~

ST-11-0009

ST-11-0009

|  |  |  |  |
|--|--|--|--|
|  |  | <p>[REDACTED] 963-1109 and [REDACTED]<br/>SV, 966-2479</p> <p><b>Revised Management Response:</b><br/>(U//FOUO) OVSC 1203: SV will work with ADET to update the FAA §702 (OVSC1203) course to reflect the amended Targeting and Minimization Procedures that the Foreign Intelligence Surveillance Court approved in September 2012. SID [REDACTED] will publish training slides onto the S2 FAA §702 Targeting Review Guidance webpage and work with ADET to update OVSC</p> <p>[REDACTED]</p> <p>(b)(3)-PLL. 86-36</p> <p>(U//FOUO) CRSK 1304 &amp; 1305:<br/>Updates to FAA §702 Practical Applications (CRSK 1304) and FAA §702 Targeting Adjudication (CRSK 1305) were completed in December 2012. In addition, enforced registration in the ELM program and targeting proficiency statistics to the individual level as well as completion rate of any required FAA §702 training (NCS) courses [REDACTED]<br/>[REDACTED] Structure OJT training will be phased in.</p> <p><b>Revised Target Completion Date:</b><br/>[REDACTED]</p> |  |
|--|--|--|--|

~~-TOP SECRET//SI//U//FORN~~~~-TOP SECRET//SI//U//FORN~~

—TOP SECRET//SI//NOFORN—

(U) This page intentionally left blank.

—TOP SECRET//SI//NOFORN—

DOCID: 42731333

—TOP SECRET//SI//NOFORN—

ST-11-0009

—TOP SECRET//SI//NOFORN—

**NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICE**



**(U//~~FOUO~~) Implementation of  
§215 of the USA PATRIOT Act and  
§702 of the FISA Amendments Act of 2008**

**ST-14-0002**

**20 February 2015**

**(U) This report might not be releasable under the Freedom of Information Act or other statutes and regulations.  
Consult the NSA/CSS Inspector General Chief of Staff before releasing or posting all or part of this report.**

**(b)(3) P.L. 86-36**

**Classified**

**Classified By:** \_\_\_\_\_

**Derived From: NSA/CSS Manual 1-52**

**Dated: 30 September 2013**

**Declassify On: 2040/02/22**

**TOP SECRET//SI//M//F//INFORN**

**(U) OFFICE OF THE INSPECTOR GENERAL**

(U) Chartered by the NSA Director and by statute, the Office of the Inspector General conducts audits, investigations, inspections, and special studies. Its mission is to ensure the integrity, efficiency, and effectiveness of NSA operations, provide intelligence oversight, protect against fraud, waste, and mismanagement of resources by the Agency and its affiliates, and ensure that NSA activities comply with the law. The OIG also serves as an ombudsman, assisting NSA/CSS employees, civilian and military.

**(U) AUDITS**

(U) The audit function provides independent assessments of programs and organizations. Performance audits evaluate the effectiveness and efficiency of entities and programs and their internal controls. Financial audits determine the accuracy of the Agency's financial statements. All audits are conducted in accordance with standards established by the Comptroller General of the United States.

**(U) INVESTIGATIONS**

(U) The OIG administers a system for receiving complaints (including anonymous tips) about fraud, waste and mismanagement. Investigations may be undertaken in response to those complaints, at the request of management, as the result of irregularities that surface during inspections and audits, or at the initiative of the Inspector General.

**(U) INTELLIGENCE OVERSIGHT**

(U) Intelligence oversight is designed to ensure that Agency intelligence functions comply with federal law, executive orders, and DOD and NSA policies. The IO mission is grounded in Executive Order 12333, which establishes broad principles under which IC components must accomplish their missions.

**(U) FIELD INSPECTIONS**

(U) Inspections are organizational reviews that assess the effectiveness and efficiency of Agency components. The Field Inspections Division is partnered with the Inspector General of the Service Cryptologic Elements and other IC entities to jointly inspect consolidated cryptographic facilities.



NATIONAL SECURITY AGENCY  
CENTRAL SECURITY SERVICE  
OFFICE OF THE INSPECTOR GENERAL



20 February 2015  
IG-11763-15  
Re-Issued

TO: DISTRIBUTION

SUBJECT: (U//FOUO) Report on the Implementation of §215 of the USA PATRIOT Act and §702 of the FISA Amendments Act of 2008 (ST-14-0002)

1. (U//FOUO) Attached please find the report on *Implementation of §215 of the USA PATRIOT Act and §702 of the FISA Amendments Act of 2008*, as requested by members of the Senate Committee on the Judiciary.
2. (U) In September 2013, ten members of the Senate Committee on the Judiciary requested a comprehensive, independent review of the implementation of §215 of the USA Patriot Act and §702 of the Foreign Intelligence Surveillance Act (FISA) Amendments Act (FAA) of 2008 (FAA §702) for calendar years 2000 through 2003. In January 2014, NSA's Office of the Inspector General (OIG) and staff from members of the Senate Committee on the Judiciary agreed on the scope of a review the OIG would conduct on NSA's use of both authorities.
3. (U) The following is the NSA OIG's report on both authorities which will be sent to the ten members of the Senate Committee on the Judiciary who requested the review, the Chairman and Ranking Member of the House Committee on the Judiciary, the Chairman and Vice Chairman of the Senate Select Committee on Intelligence, and the Chairman and Ranking Member of the House Permanent Select Committee on Intelligence.
4. (U//FOUO) We appreciate the cooperation and courtesies extended to our personnel throughout the review.

The signature is handwritten in cursive ink. It appears to read "George Ellard".  
 DR. GEORGE ELLARD  
 Inspector General

(U) This report might not be releasable under the Freedom of Information Act or other statutes and regulations. Consult the NSA/CSSSI Inspector General's Chief of Staff before releasing or posting all or part of this report.

(U//FOUO) DISTRIBUTION  
SND DIR (Ron Morris)  
TD DIR [REDACTED]  
OGC (Raj De)

AIG [REDACTED] f! t! n! •n

CLPO (Rebecca Richards)..

ODOC (Catherine Aucella)

LAO (Ethan Bauman)

OGC [REDACTED]

S0 [REDACTED]

S1 [REDACTED]

S1S [REDACTED]

S2 [REDACTED]

S2I [REDACTED]

S3 [REDACTED]

S313 [REDACTED]

DL S02 frontoffice  
S01 S02 frontoffice ALIAS

S02 [REDACTED]

S1 [REDACTED]

S1S [REDACTED]

S205 [REDACTED]

S2b3 [REDACTED]

S2D [REDACTED]

S2M [REDACTED]

S3 [REDACTED]

S31324 [REDACTED]

S3409 [REDACTED]

S35411 [REDACTED]

S35423 [REDACTED]

S35433 [REDACTED]

DL BMD\_Weekly(ALIAS)SSTCI  
DL SIDIGLIAISON  
DL TD\_REGISTRY  
DL TD\_Strat\_Ops\_Grp  
DL D\_COMPLY\_TASKER  
DL d\_gc\_registry  
DL d\_lao\_tasker

IG  
D/IG  
DII [REDACTED]  
DII, D12, D13, D14

## (U) TABLE OF CONTENTS

|   |     |
|---|-----|
| I. (U) INTRODUCTION .....   | ii  |
| (U) REASON FOR REVIEW .....   | ii  |
| (U) OBJECTIVES .....  | ii  |
| II. (U) SECTION 215 OF THE USA PATRIOT ACT .....                                    | 1   |
| (U) BACKGROUND .....  | 1   |
| (U) METHODOLOGY AND SCOPE .....   | 2   |
| (U) BR FISA PROGRAM CONTROL FRAMEWORK .....   | 3   |
| (U) BR FISA PROGRAM INCIDENTS OF NON-COMPLIANCE .....                               | 56  |
| (U) NSA USE OF THE BR FISA AUTHORITY .....  | 63  |
| III. (U) FAA §702 .....   | 70  |
| (U) BACKGROUND .....  | 70  |
| (U) METHODOLOGY AND SCOPE .....   | 71  |
| (U) FAA §702 PROGRAM CONTROL FRAMEWORK .....  | 72  |
| (U) FAA §702 INCIDENTS OF NON-COMPLIANCE .....                                      | 136 |
| (U) NSA USE OF THE FAA §702 AUTHORITY .....   | 143 |
| IV. (U) ABBREVIATIONS AND ORGANIZATIONS .....                                       | 150 |
| (U) APPENDIX A: ABOUT THE §215 AND FAA §702 REVIEW .....                            | 153 |
| (U) APPENDIX B: BR FISA PROGRAM CHANGES 2010-2012 .....                             | 157 |
| (U) APPENDIX C: BR FISA PROGRAM INCIDENTS OF NON-COMPLIANCE 2010 THROUGH 2012 ..... | 159 |
| (U) APPENDIX D: FAA §702 PROGRAM CHANGES .....                                      | 160 |

## I. (U) INTRODUCTION

### **(U) Reason for Review**

(U) In September 2013, ten members of the Senate Committee on the Judiciary requested a comprehensive, independent review of the implementation of §215 of the USA PATRIOT Act and §702 of the Foreign Intelligence Surveillance Act (FISA) Amendments Act (FAA) of 2008 for calendar years 2010 through 2013.

### **(U) Objectives**

(U) In January 2014, the National Security Agency/Central Security Service (NSA/CSS) Office of the Inspector General (OIG) and Committee staff agreed that the NSA OIG would review NSA's implementation of both authorities for calendar year 2013. The study has three objectives:

#### **(U) Objective I**

- (U) Describe how data was collected, stored, analyzed, disseminated, and retained under the procedures for §215 and FAA §702 authorities in effect in 2013 and the steps taken to protect U.S. person information.
- (U) Describe the restrictions on using the data and how the restrictions have been implemented, including a description of the data repositories and the controls for accessing data.
- (U) Describe oversight and compliance activities performed by internal and external organizations in support of §215 Foreign Intelligence Surveillance Court (FISC) Orders and FAA §702 minimization procedures.

#### **(U) Objective II**

- (U) Describe incidents of non-compliance with §215 FISC Orders and FAA §702 Certifications and what NSA has done to minimize recurrence.

#### **(U) Objective III**

- (U) Describe how analysts used the data to support their intelligence missions.

**(U//FOUO)** Our study of NSA's implementation of §215 and FAA §702 authorities was based largely on program stakeholder interviews and reviews of policies and procedures and other program documentation. For this review, the NSA OIG documented the controls implemented to address the requirements of each authority; however, we did not verify through testing whether the controls were operating as described by program stakeholders.

~~TOP SECRET//SI//NOFORN~~

ST-14-0002

**II. (U) SECTION 215 OF THE USA PATRIOT ACT****(U) Background****(U) Business Records Order**

(U) Since May 2006, the Foreign Intelligence Surveillance Court (FISC) has authorized the National Security Agency/Central Security Service's (NSA) bulk collection program under the "business records" provision of the Foreign Intelligence Surveillance Act (FISA), 50 U.S.C. § 1861, as amended by § 2155 of the USA PATRIOT Act, legislation enacted by the US Congress and signed into law by the President. From its first authorization in May 2006 through December 2014, the program has been approved 40 times under Business Records (BR) Orders issued by 18 FISC judges.

(b)(1)  
(b)(3)-P.L. 86-36  
(b)(3)-50 USC 3024(i)

~~(CTNSC 04/17)~~ Pursuant to the series of BR Orders issued by the FISC, NSA receives certain call detail records (or BR metadata) from ~~D~~ U.S. telecommunications providers. NSA refers to the series of BR Orders approved by the FISC as the "BRR Order" and the control framework NSA has implemented as the "BRR FISA program."

(U) The BR Order requires that providers produce to NSA certain information about telephone calls, principally those made within the United States and between the United States and foreign countries. This information is limited to BR metadata, which includes information concerning telephone numbers used to make and receive calls, when the calls took place, and during the call last duration, but does not include information about the content of calls, the names of the participants, or call site location information (CSLI).

(U) The BRR FISA program was developed to assist the U.S. government in detecting communications between known or suspected terrorists who are operating outside the United States and communicating with other individuals in the United States, as well as communications between operatives within the United States. The BRR Order authorizes NSA analysts to query BR metadata only for identified counterterrorism purposes. The BRR FISA program includes oversight mechanisms to maintain compliance with the BRR Order and external reporting requirements to the FISC and Congress.

**(U) BR renewal process**

(U) Approximately every 90 days, the Department of Justice (DoJ) on behalf of the Federal Bureau of Investigation (FBI) and NSA files an application with the FISC requesting that certain providers continue to provide calling records to NSA for another 90 days. If the FISC approves the government's applications to renew the program, the Court issues a "primary order" delineating the scope of what the providers must furnish to NSA and the provisions for NSA's handling of BR

~~TOP SECRET//SI//NOFORN~~

metadata. The FISC issues "secondary orders" separately to each provider, directing them to deliver an electronic copy of certain calling records to NSA daily until the expiration of the BR Order.

### (U) Methodology and Scope

---

(U) Our review of the BR FISA program control framework incidents of non-compliance, and NSA's use of the authority to support its counterterrorism (CT) mission was based largely on BR program stakeholder interviews and reviews of policies and procedures and other program documentation. For this review, we did not verify through testing whether the controls were operating as described by BR program stakeholders. However, we tested controls of the BR program during previous NSA Office of the Inspector General (OIG) reviews (see the Oversight section for a list of those reviews).

(b)(3)-P.L. 86-36

(U) Our study focused on the processes and controls in place in 2013. We used BR Order 13-158, approved by the FISC [redacted]

[redacted] and compared the requirements listed in that Order with the processes and controls NSA used to maintain compliance with that Order. In addition, we documented the changes implemented in the BR FISA program following the President's directives in 2014.

### (U) Presidential directives affecting querying controls in 2014

(U) On 17 January and 27 March 2014, the President of the United States directed that NSA implement the following changes to the BR FISA program:

1. (U//FOUO) Submit selection terms to the FISC for reasonable articulable suspicion (RAS) approval (see Querying section for RAS discussion). Before 17 January 2014, RAS selection terms were approved by the Chief or Deputy Chief of NSA's Homeland Security Analysis Center (S214) or one of the twenty specially authorized Homeland Mission Coordination (HMC) cells the BR Order required and NSA's Office of General Counsel (OGC) performed First Amendment reviews for selection terms associated with US Persons (USPs).
2. (U//FOUO) Restrict contact chaining to two hops from seed selection terms (see Querying section for contact chaining discussion). Before 17 January 2014, the BR Order authorized appropriately trained and authorized NSA analysts to query to three hops; however, NSA guidance restricted those analysts to query BR FISA repositories two hops from seed selection terms and one additional hop (three hops from seed selection terms) with Analysis and Production (S2) management approval.
3. (U) Store BR metadata in provider controlled repositories and not in NSA repositories. Once implemented, NSA will submit FISC-approved RAS selection terms to providers for them to query their repositories. Providers will provide to NSA only the results of those queries.

~~TOP SECRET//SI//NOFORN~~

ST-14-0002

(U//~~FOUO~~) NSA implemented the first two directives by February 2014. The third directive, storing BR metadata in provider repositories and maintaining only those query results from providers, will require Congression approval of a new statute for the production of business records, which had not been implemented before this report was issued.

(U//~~FOUO~~) The following sections describe how the BR FISA program control framework complies with BR Order 13-158 (including the changes implemented following the President's directives in 2014), the 2013 BR FISA program incidents of non-compliance, and NSA's use of the BR FISA authority.

## **(U) BR FISA Program Control Framework**

---

(U//~~FOUO~~) The BR FISA program control framework describes how NSA collects, samples, stores, accesses, queries, disseminates, and retains BR metadata and the oversight mechanisms to comply with the BR Order. This section summarizes the provisions of the BR Order and the controls implemented for each phase of the BR FISA production cycle.

### **(U) Collection**

#### **(U) Provisions of BR Order 13-158**

(~~DISSEMINATE~~) The BR Order requires [ ] U.S. telecommunications providers to provide [ ] an electronic copy of certain call detail records (hereinafter referred to as "BR metadata"). The BR Order defines BR metadata as comprehensive communications routing information including but not limited to session identifying information (e.g., originating and terminating telephone number, International Mobile Subscriber Identity (IMSI) number, and International Mobile Equipment Identity (IMEI) number), subscriber identifier, telephone calling account numbers, and the time and duration of call.<sup>1</sup> BR metadata does not include the substantive content of communications (the name and address, financial information of a subscriber or customer; or CSLI).

(b)(1)

(b)(3)-P.L. 86-366

(b)(3)-50 USC 3024(i)

#### **(U) Data received from providers**

~~(b)(4) ~ ~ ~~~~~[ ]~~

<sup>1</sup> (U) The IMEI number is a type of metadata related to mobile telephony. It is permanently embedded in a mobile telephone handset by the manufacturer and generally is not changeable by the user. In most instances, the IMEI does not travel with the Subscriber Identity Module (SIM) card, in contrast to the IMSI number, which does. The IMSI number is another type of metadata related to mobile telephony. It is a 15-digit number used to identify a customer. IMSI numbers are permanently stored on SIM cards, allowing a user to plug a card into any mobile telephone and be billed correctly. Calling card numbers are numbers used for billing telephone calls. A calling card number may be a telephone number, as the phrase is commonly understood and used, plus a personal identification number, or may be another unique set of numbers not including a telephone number.

~~TOP SECRET//SI//NOFORN~~

~~TOP SECRET//SI//NOFORN~~

ST-14-0002

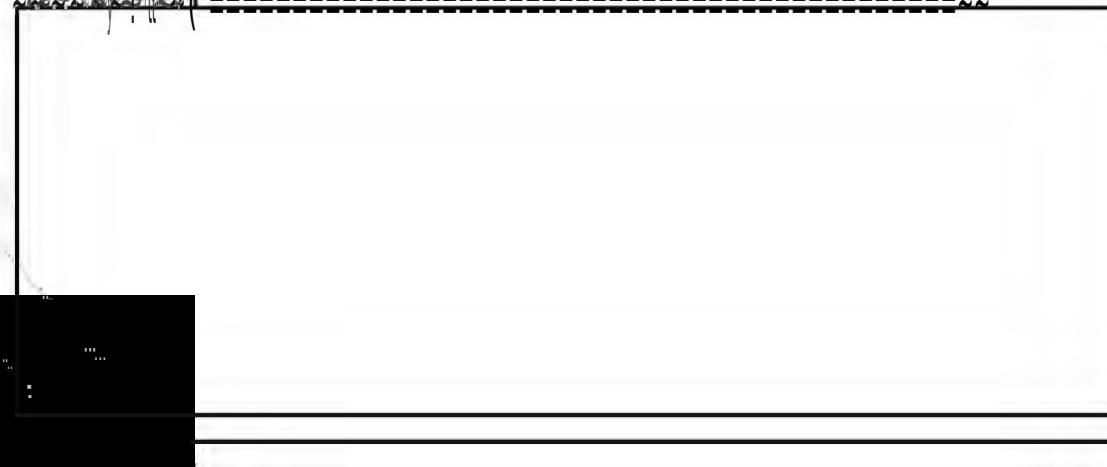


(TS//SI//NF)



(b)(1)  
(b)(3)-P.L. 86-36  
(b)(3)-50 USC 3024(i)

(TS//SI//NF)



(TS//SI//NF)



<sup>2</sup> (U//FOUO) A SCIF is an accredited area, room, or installation, incorporating physical control measures (e.g., barriers, locks, alarm systems, armed guards), to which no person has authorized access unless approved to receive the particular category of sensitive compartmented information and has a need to know the sensitive compartmented information activity conducted therein.

(b)(3)-P.L. 86-36

<sup>3</sup> (U//FOUO) [redacted] A contact chain shows that selection term A communicated with selection term B, their first and last contact dates, telephony type, and the total number of communications between selection terms A and B.

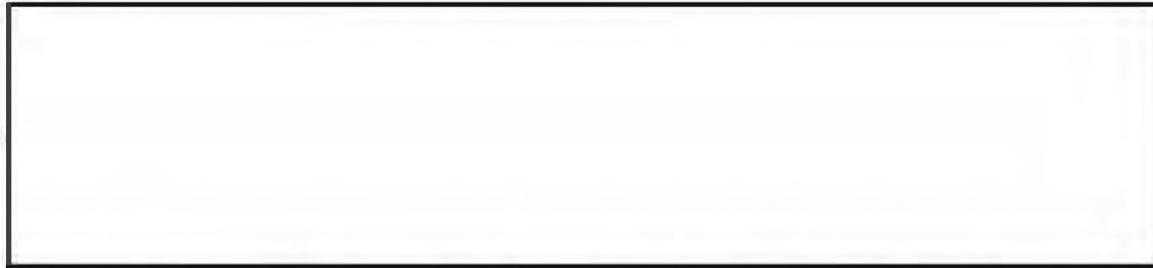
<sup>4</sup> (C//REL TO USA, FVEY) [redacted]

(b)(1)  
(b)(3)-P.L. 86-36  
(b)(3)-50 USC 3024(i)

~~TOP SECRET//SI//NOFORN~~

~~TOP SECRET//SI//NOFORN~~

ST-14-0002



(b)(1)

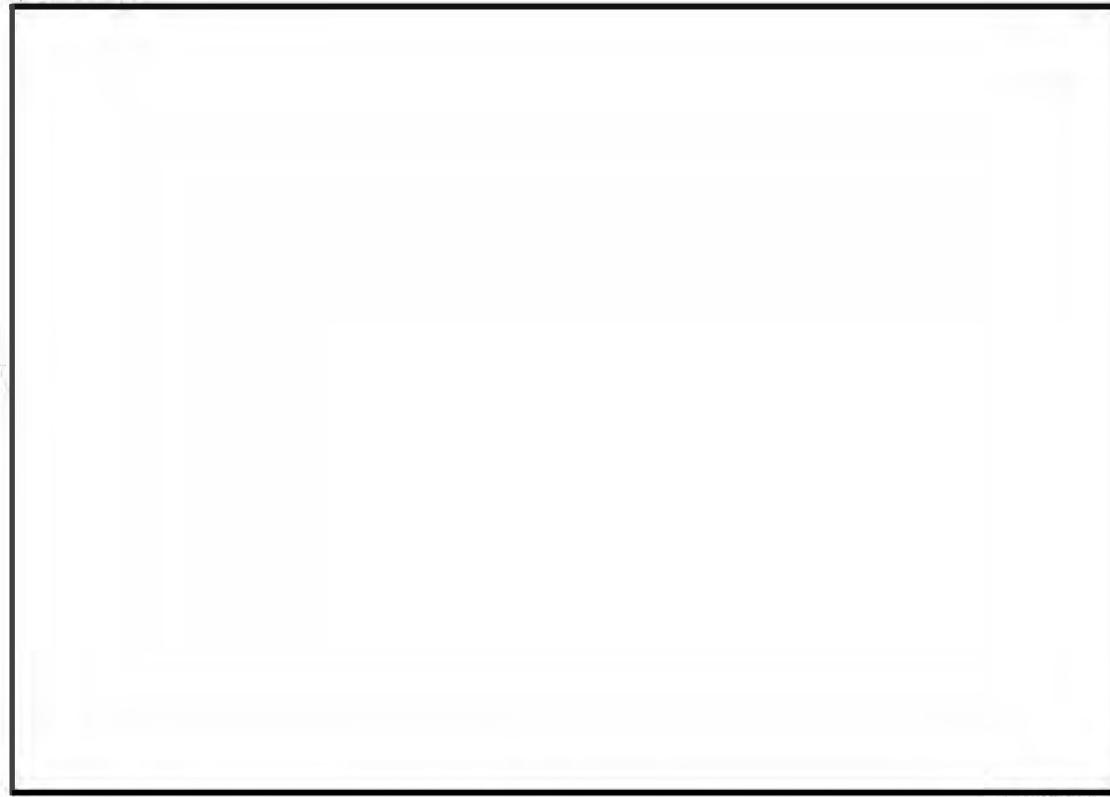
(b)(3)-P.L. 86-36

(b)(3)-50 USC 3024(i)

(TS//SI//NF) Figure 1 illustrates the BR metadata dataflow from the provider to NSA and the various BR metadata repositories in 2013.

(TS//SI//NF) Figure 1. BR Metadata Dataflow and Repositories

(TS//SI//NF)



(TS//SI//NF)

(TS//SI//NF) The BR Order requires that [REDACTED] provide all BR metadata [REDACTED] for communications between the United States and abroad or wholly within the United States, including local telephone calls. The BR Order does not require [REDACTED]

(b)(1)

(b)(3)-P.L. 86-36

(b)(3)-50 USC 3024(i)

(TS//SI//NF)

~~TOP SECRET//SI//NOFORN~~

-TOP SECRET//SI//NOFORN

ST-14-0002

(b)(1)  
(b)(3)-P.L. 86-36  
(b)(3),50 USC 3024(i) (TS//SI//NF)

(U) Table 1: BR FISA [REDACTED]

(b)(3)-P.L. 86-36

(TS//SI//NF)

(TS//SI//NF)

**(U) Metadata Sampling****(U) Sampling to verify BR metadata integrity**

(U//FOUO) NSA's Data Integrity Analysts (DIAs) team [REDACTED] (S31324) has [REDACTED] full-time employees dedicated to the BR FISA program. DIA responsibilities include:

<sup>6</sup> (U//FOUO) The BR FISA Authority Lead is responsible to the NSA Director and the Director of the Signals Intelligence Directorate for implementation of FISC BR authorizations by the NSA organizations responsible for the collection, processing and analysis of BR metadata under the BR Order.

-TOP SECRET//SI//NOFORN

~~TOP SECRET//SI//NOFORN~~

ST-14-0002

- (U//FOUO) Verifying that BR metadata is correctly ingested, processed and formatted into chains;
- (U//FOUO) [REDACTED] (b)(3)-P.L. 86-36
- (U//FOUO) [REDACTED]
- (S//NF) [REDACTED] (b)(1)  
(b)(3)-P.L. 86-36
- (S//NF) [REDACTED] (b)(3)-P.L. 86-36
- (S//NF) [REDACTED] (b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36

(TS//SI//NF) NSA has two types of controls to monitor data received from the providers and maintain compliance with the BR Order. The first is [REDACTED] preventive control that uses [REDACTED] rules. The second is a [REDACTED] performed by the DIAs using data sampling techniques [REDACTED]

(b)(1)  
(b)(3)-P.L. 86-36

(TS//SI//NF)

(b)(3)-P.L. 86-36

changes are  
project

team runs tests to verify that [REDACTED] changes have been implemented and provides the test results to the DIA team to validate that the changes have been made.

(U//FOUO) Sampling DIAs run [REDACTED] queries on the BR metadata to answer five questions as part of the sampling process (Controls) Verify Compliance with the BR Order:

<sup>7</sup> (U//FOUO) The standard format is [REDACTED]

(b)(3)-P.L. 86-36

~~TOP SECRET//SI//NOFORN~~

TOP SECRET//SI//NOFORN

ST-14-0002

1. (TS//SI//NF) Did the BR metadata contain credit card numbers?
2. (U//FOUO) Did NSA detect CSLI in the [redacted], ~ [redacted] identification field? (b)(1)  
(b)(3)-P.L. 86-36
3. (U) Did the BR metadata record structure adhere to expectations?
4. (U) Did the BR metadata record content adhere to expectations?
5. (U//FOUO) Did [redacted] adhere to expectations?

(U) The sampling results are submitted to NSA's Office of the Director of Compliance (ODOC) in weekly BR FISA compliance reports. ODOC compiles the information with other compliance reports and provides it to the Director of Compliance for review. The BR FISA Authority Lead summarizes the weekly BR FISA compliance reports for the DoJ National Security Divisions (NSD) review before quarterly compliance review meetings (see Oversight section).

(TS//SI//NF) Credit card numbers [redacted] DIAAs sample the [redacted] known to have contained credit card numbers used as part of calling card personal identification numbers. The BR Order does not authorize NSA to receive customer financial information [redacted]. [redacted] DIAAs sample all BR metadata records for the [redacted] that could contain credit card numbers. The sampling of BR metadata is performed to identify [redacted] to screen for credit card numbers.

When specific [redacted] are identified, DIAAs try to [redacted]

(TS//SI//NF) [redacted]  
[redacted] DIAAs identify them as credit card numbers and forward them to [redacted]. As determined whether the credit card numbers were registered into [redacted] and notifies stakeholders, including DoJ NSD. (b)(1)-P.L.  
(b)(3)-P.L. 86-36 (b)(3)-P.L. 86-36

(TS//SI//NF) To demonstrate the number of files and BR metadata records that are sampled daily for credit cards, the OIG randomly selected [redacted] for review (Table 2).

TOP SECRET//SI//NOFORN

TOP SECRET//SI//NOFORN

ST-14-0002

## (U) Table 2 [redacted] Sampling Metrics for Credit Cards

(TS//SI//NF)

(b)(1)  
 (b)(3)-P.L. 86-36  
 (b)(3)-50 USC 3024(i)

(TS//SI//NF)

## (U) Table 3 [redacted] Sampling Metrics for Credit Cards

(TS//SI//NF)

(TS//SI//NF)

(TS//SI//NF)

(b)(1)  
 (b)(3)-P.L. 86-36  
 (b)(3)-50 USC 3024(i)

J

(TS//SI//NF) Cell site location information (CSLI) DIAs test the [redacted] to verify that it does not contain CSLI because the BR Order prohibits NSA from receiving this data. The DIAs sample [redacted]

(b)(3)-P.L. 86-36

[redacted] DIAs have identified no CSLI data in [redacted] since it became operational [redacted] (1)(2)-P.L. 86-36  
 (b)(3)-P.L. 86-36

(TS//SI//NF) Record structure The DIAs sample BR metadata records [redacted] each feed to test whether the BR metadata record structure has changed [redacted]

TOP SECRET//SI//NOFORN

(b)(1)  
(b)(3)-P.L. 86-36

If any tests show differences, a warning message is generated for the DAs to address. Changes in BR metadata record structure are very rare but, if identified, the provider is contacted to determine whether the change is permanent or a one-time processing anomaly.

(U//FOUO) BR metadata record content DAs review the BR metadata record content for each feed [redacted]

<sup>8</sup> According to the DAs, exceptions are very rare.

(b)(3)-P.L. 86-36

(U//FOUO) Table 4 shows the percentage of the [redacted] feeds tested for BR metadata record structure and content during 2013.

(U//FOUO) Table 4-15 Sampling Percentages for BR Metadata Record Structure and Content Testing

(TS//SI//NF)

{6}(1f)  
(b)(1)  
(b)(3)-P.L. 86-36  
(b)(3)-50 USC 3024(i)

(TGM/NF)

(TS//SI//NF) Data feed volumes DAs monitor data feed volumes [redacted] for anomalies by reviewing the [redacted] "Status Report," which lists for each feed the number of raw BR metadata records [redacted] received and the number of [redacted] records [redacted]

(b)(3)-P.L. 86-36

(b)(1)  
(b)(3)-P.L. 86-36

(U//FOUO) Table 5 shows the number of BR metadata records received [redacted]

<sup>8</sup> (U//FOUO) BR metadata record content is distinct from the content of communications: BR metadata record content does not contain the content of communications defined in 18 U.S.C. §2510, as the substance, purport, or meaning of a communication.

~~TOP SECRET//SI//NOFORN~~

ST-14-0002

## (U) Table 5. Total Number of BR Metadata Records Received [redacted] D

(b)(3)-P.L.866366

(TS//SI//NF)

(TS//SI//NF)

(U) Table 6 summarizes the provisions of BR Order 13-158 for collection and the controls NSA implemented to maintain compliance.

(b)(1)

(b)(3)-P.L.866366

(b)(3)-50 USC 3024(i))

## (U) Table 6. Collection Provisions and Controls

(TS//SI//NF)

(TS//SI//NF)

| Provision                                      | Control  |
|--|--|
| (TS//SI//NF) Provide Daily BR Metadata Records | (TS//SI//NF) [redacted] monitored [redacted] for data flow problems. DIAs monitor data feed volumes [redacted] for anomalies.  |
| (U) NSA Only Receives Authorized Data          | (TS//SI//NF) Parser rules are designed to prevent unauthorized data from being ingested into operational systems. DIAs sample data [redacted] to detect unauthorized data. |

(b)(1)

(b)(3)-P.L.866366

## (U) Repositories

## (U) Provisions of BR Order 13-158

(U) NSA will store and process BR metadata in repositories within secure networks under NSA control.

## (U) NSA repositories that store BR metadata

(U//FOUO) All NSA systems that store and process BR metadata are certified as secure through an accreditation and certification process and are in NSA controlled SCIFs. During 2013, the following systems stored and processed BR metadata.

(b)(3)-P.L.866366

- (S//SI//REL TO USA, FVEY) [redacted] is the corporate contact claiming database [redacted] 1 [redacted] 1

(b)(1)

(b)(3)-P.L.866366

(b)(3)-50 USC 3024(i))

~~TOP SECRET//SI//NOFORN~~

orate database

- (U//~~FOUO~~) [REDACTED] is the contingency system for [REDACTED] and has the same hardware and software as [REDACTED]
- (S//REL TO USA, FVEY) [REDACTED] is the system backup [REDACTED]
- (U//~~FOUO~~) Backup tapes are maintained at [REDACTED] The BR metadata electronically stored in [REDACTED] are saved to tape backup [REDACTED]
- (U//~~FOUO~~) [REDACTED] designed for the BR FISA program is software that runs on a [REDACTED] system. The BR FISA program is software
- (U//~~FOUO~~) [REDACTED] data distribution systems move BR metadata between NSA systems.

(S//REL TO USA, FVEY) How information is stored in [REDACTED]

(S//REL TO USA, FVEY) [REDACTED] are the only operational databases used to store BR metadata for intelligence analysis. As previously mentioned, [REDACTED]

(b)(1)  
(b)(3)-P.L. 86-36

(BS//SI//NF) [REDACTED]

(b)(1)  
(b)(3)-P.L. 86-36  
(b)(3)-50 USC 3024(ii)

(b)(3)-P.L. 86-36

(U//~~FOUO~~) [REDACTED]

~~-TOP SECRET//SI//NOFORN~~

ST-14-0002

(U//FOUO) Figure 2. [REDACTED] Architectures (b)(3)-P.L. 86-36

~~(TS//SI//NF)~~

(b)(1)  
(b)(3)-P.L. 86-36  
(b)(3)-50 USC 3024(i)

~~(TS//SI//NF)~~

(b)(1)  
(b)(3)-P.L. 86-36  
(b)(3)-18 USC 798  
(b)(3)-50 USC 3024(i)

~~(TS//SI//NF)~~**(U) NSA system accreditation and certification processes**

(U//FOUO) Accreditation [REDACTED] (TS) is responsible for managing the risk on all NSA networks and the computer systems and devices connected to those networks. TS responsibilities include:

(b)(3)-P.L. 86-36

<sup>10</sup> (U) A relational database stores data in tables using a standardized data format. This allows similar information to be organized and queried on the basis of specific data fields.

~~-TOP SECRET//SI//NOFORN~~

- (U//~~FOUO~~) Guiding prioritizing and overseeing the development of information assurance programs necessary to ensure protection of information systems and networks by managing the NSA Information Security Program,
- (U//~~FOUO~~) Serving as the NSA Director's Authorizing Official to accredit all NSA information systems,
- (U//~~FOUO~~) Conducting information systems security and accreditation and risk management programs, and
- (U//~~FOUO~~) Establishing maintaining and enforcing information systems security policies and implementation guidelines for NSA.

(U//~~FOUO~~) Accreditation is the official management decision to permit operation of an information system in a specific environment at an acceptable level of risk, based on the implementation of an approved set of technical, managerial, and procedural safeguards.

(U//~~FOUO~~) When accrediting systems, TS uses a risk management framework to determine the appropriate level of risk mitigation needed to protect systems, information, and infrastructure. This framework comprises six steps.

- (U) Categorize the information and information system,
- (U) Select an initial baseline of security controls and tailor as appropriate for the system, data, and environment,
- (U) Implement and build the security controls into the information system,
- (U) Authorize the operation of the information system (accept the risk), and
- (U) Monitor continually and assess the effectiveness of the security controls.

(U//~~FOUO~~) Before a system is authorized to be put on a network, it must go through the accreditation process and be approved by TS. Table 7 lists the date through which the BR repositories are accredited.

**(U) Table 7. Dates through which BR Repositories Are Accredited**

(C//REL TO USA, FVEY)

| Repository                       | Accredited Through | [REDACTED] |
|----------------------------------|--------------------|------------|
| (b)(1)<br>(b)(3)-P.L.866366<br>t |                    |            |

(C//REL TO USA, FVEY)

(U//~~FOUO~~) **Certification** In addition to the TS system accreditation requirement, all systems containing FSA data must be certified by [REDACTED] (CIV) [REDACTED] (LV4). TY4 is the NSA authority for certification of systems to ensure they are compliant with the legal and policy regulations protecting USP privacy.

(b)(3)-P.L.866366

~~TOP SECRET//SI//NOFORN~~

ST-14-0002

(U//~~FOUO~~) [REDACTED] TV began certifying FISA systems, including the repositories that contain BR metadata, to ensure that they comply with USP privacy protection. TV developed [REDACTED] the NSA corporate database for registration of NSA systems and their compliance certification and data flows. It is NSA's authoritative source of all compliance certifications. TV's certification process evaluates system controls for maintaining compliance in the following areas: purge, data retention and aging off, data access, querying, dissemination, data tagging, targeting, and analytical processes.

(b)(3)-P.L. 86-36  
(b)(6)

(U//~~FOUO~~) To be certified to handle FISA data, systems must be certified by TV as part of the Compliance Certification process. Table 8 shows the TV4 certification dates for repositories that contain BR metadata.

**(U) Table 8. Certification Dates for Repositories Containing BR Metadata**

(C)REF TO USA, FVEY)

| Repository | Date Certified |
|------------|----------------|
| [REDACTED] | [REDACTED]     |

(C)REF TO USA, FVEY)

(U) Table 9 summarizes the provisions of BR Order 13-158 for repositories under the control NSA implemented to maintain compliance.

**(U) Table 9. BR Repository Provision and Control**

(U//~~FOUO~~)

| Provision  | Control   |
|--|---|
| NSA will store and process BR metadata in repositories within secure networks under NSA control. | All BR FISA systems are certified as secure through NSA's system accreditation (TSS) and certification process (TV4) and located in NSA controlled SCIFs. |

(U//~~FOUO~~)

### **(U) Access and Training**

#### **(U) Provisions of BR Order 13-158**

(U) BR metadata shall carry unique markings such that forward and other controls (including user authentication services) can restrict access to authorized personnel who have received appropriate and adequate training in legal and this authority. NSA shall restrict access to BR metadata to authorized personnel who have received appropriate and adequate training.

(U) Appropriately trained and authorized technical personnel may access the BR metadata to perform the processes needed to make it usable for intelligence analysis. The Court understands that the technical personnel responsible for NSA's underlying corporate infrastructure and transmission of the BR metadata from the

~~TOP SECRET//SI//NOFORN~~

specified persons to NSA will not receive special training regarding the authority granted herein.

(U) NSA's OGC and [ ] will further ensure that all NSA personnel who receive query results in any form first receive appropriate and adequate training and guidance regarding the procedures and restrictions for the handling and dissemination of such information. NSA will maintain records of all such training.

(U) OGC will provide DDCI/NSSD with copies of all formal briefing and/or training materials (including all revisions) used to brief or train NSA personnel concerning this authority.

**(U) Restricting access to BR metadata to authorized personnel**

(TS//SI//NF) The Signals Intelligence Directorate's (SID) Office of Oversight & Compliance (SV) verifies semi-weekly that personnel with [ ] maintain the required credentials [ ]

[ ] The training required for these two credentials is listed in the "Appropriate and Adequate Training" heading of this section. [ ] (b)(1)

(TS//SI//NF) The [ ] credential signifies that an individual has been adequately and appropriately trained (discussed below) with regard to the BRFISA program and provides the authorization to view the results of BR metadata queries, in any form, including written and oral summaries of results. [ ] does not provide access to the BR metadata in the bulk metadata (BRMD) repository or an authorization to query the data. (b)(3)-P.L. 86-36

(TS//SI//NF) Table 10 shows a breakdown of the number of personnel with [ ] as of 31 December 2013 by affiliation. (b)(1) (b)(3)-P.L. 86-36

**(TS//SI//NF) Table 10. Number of Personnel with [ ] by Affiliation**

(TS//SI//NF)

| Affiliation          |   |
|----------------------|---|
| NSA Civilians        | 1 |
| NSA Military         |   |
| Non-Agency Civilians |   |
| Contractors          |   |
| Total                |   |

(TS//SI//NF)

(TS//SI//NF) Table 11 shows a breakdown of the number of personnel with [ ] as of 31 December 2013 by work role.

~~TOP SECRET//SI//NOFORN~~

ST-14-0002

(b)(1)

(b)(3)-P.L.86-36

~~(TS//SI//NF)~~ Table 11. Number of Personnel with [ ] by Work Role~~(TS//SI//NF)~~

| Work Role  | Number of Personnel |
|------------|---------------------|
| Analyst    |                     |
| Oversight  |                     |
| Leadership |                     |
| Staff      |                     |
| Technical  |                     |
| Contractor |                     |
| Total      |                     |

~~(TS//SI//NF)~~

(b)(3)-P.L. 86-36

~~(TS//SI//NF)~~ The [ ] credential signifies that a person is authorized to access BMD repositories and is the first step in obtaining the ability to use [ ] to perform queries against BR metadata. [ ] is only authorized for specific intelligence analysts working CT targets described in the BR Order and technical personnel who maintain the systems that process and store BR metadata. The BR FISA Authority Lead is the ultimate authority for deciding which organizations are authorized to access BR metadata repositories.

(b)(1)  
(b)(3)-P.L. 86-36

~~(TS//SI//NF)~~ Table 12 shows a breakdown of the number of personnel with [ ] as of 31 December 2013, by affiliation and work role.

(b)(1)

(b)(3)-P.L. 86-36

~~(TS//SI//NF)~~

| Affiliation and Work Role | Number of Personnel |
|---------------------------|---------------------|
| NSA Civilian              |                     |
| - Analyst                 |                     |
| - Oversight               |                     |
| - Technical               |                     |
| - Total                   |                     |
| NSA Military              |                     |
| Contractors               |                     |
| - Technical               |                     |
| Total                     |                     |

~~(TS//SI//NF)~~

~~(TS//SI//NF)~~ [ ] In addition to [ ] If an individual needs to query BR metadata using the intelligence analyst contact chaining tool, a Division Chief, Deputy Division Chief, Branch Chief, or Deputy Branch Chief must submit to SV a written request that the individual be given query access. If the individual is current in all training and holds the [ ] credentials, SV sends an e-mail to the [ ] team and requests that the person be added to the [ ]

(b)(3)-P.L. 86-36

<sup>11</sup> (U//FOUO) [ ] is the graphical user interface analysts use to query data, including BR metadata, in [ ]

~~TOP SECRET//SI//NOFORN~~

TOP SECRET//SI//NOFORN

ST-14-0002

[redacted] User Group in [redacted]<sup>12</sup>. The [redacted] administrator verifies the person's credentials and training, adds the person to the user group, and notifies SV when complete. Upon completion, [redacted] automatically sends an e-mail to SV indicating that the person has been added to the user group. This additional management control helps ensure that only appropriately trained and authorized personnel are able to execute queries.

(b)(3)-P.L. 86-36

(U//FOUO) Table 13 shows a breakdown of the number of personnel on the [redacted] User Group with querying capability as of 31 December 2013.

(b)(3)-P.L. 86-36

(U) **Table 13. Number of Personnel with Querying Capability as of 31 December 2013**

(U//FOUO)

| Work Role    | Number of Personnel |
|--------------|---------------------|
| Analysts     | [redacted]          |
| Technical    | [redacted]          |
| <b>Total</b> | [redacted]          |

(U//FOUO)

(TS//SI//NF) **Receiving query results** NSA personnel who receive query results are required to receive training and guidance regarding the procedures and restrictions for handling and disseminating such information. Before analysts send BR-unique query results containing USPP information to another individual, they must first confirm that the recipient has the [redacted] credential.<sup>13</sup> Sharing BR-unique query results containing USP information with an individual without the [redacted] credential would violate the BR Order and require notice to the Court.

(b)(1)

(b)(3)-P.L. 86-36

(U) **Training records** The BR Order requires that NSA maintain records of BR training. NSA's Associate Directorate for Education and Training (ADET) Enterprise Learning Management Database is NSA's source system of record (SSSR) for maintaining training completion records for all required training.

(U) Figure 3 shows the categories of individuals authorized access to BR data.

(b)(3)-P.L. 86-36

<sup>12</sup> (U//FOUO) [redacted] is NSA's Corporate Authorization Service Portal, which provides authentication attributes and access control services to NSA programs and projects.

<sup>13</sup> (U//FOUO) [redacted]

TOP SECRET//SI//NOFORN

TOP SECRET//SI//NOFORN

ST-14-0002

(U//~~FOUO~~) Figure 3. Access to BR Information Determined by Credentials Maintained by BR Stakeholders

(b)(1)  
 (b)(3)-P.L. 86-36


~~(TS//SI//NF)~~ Obtaining the credential To obtain the [REDACTED]

a request must be submitted in the [REDACTED] -1  
 NSA's corporate credentialing system. A [REDACTED] request must contain the name of a valid sponsor who currently holds the requested credential. The Associate Directorate for Security and Counterintelligence (Q) reviews [REDACTED] requests for security concerns. If approved, the request is forwarded to SV for final adjudication. SV verifies that the individual is current on the required training (explained below) and that the request includes a valid mississippijustification. If all requirements are met, SV approves the credential in [REDACTED] for entry into [REDACTED]

(b)(1)  
 (b)(3)-P.L. 86-36

~~(TS//SI//NF)~~ Maintaining the credential To ensure that personnel remain current on training, SV runs a [REDACTED] report several times a week that lists all the personnel with the [REDACTED] credential and their training status which is color coded (green=current, red=expired). If someone's OVSC1000 or OVSCI100 training has expired, SV notifies that person by e-mail that training must be completed. If OVSC1800 or OVSCI1205/OVSCI1206 has expired, access is revoked immediately. Access is not restored until a new [REDACTED] request is submitted and all training is current. If an individual's training expires and the credential has been revoked, this would not violate the BR Order. However, if someone accesses BR metadata but has not completed the required training this would violate the BR Order because the person has not been appropriately and adequately trained. The violation requires notice to the Court.<sup>14</sup>

<sup>14</sup> (U//~~FOUO~~) The Court understands that the technical personnel responsible for NSA's underlying corporate infrastructure and the transmission of the BR metadata from the specified persons to NSA will not receive special training regarding the authority granted herein.

TOP SECRET//SI//NOFORN

(U//~~FOUO~~) Appropriate and adequate training NSA/CSS Policy 1-23, *Procedures Governing NSA/CSS Activities That Affect U.S. Persons*, 30 July 2013, requires that Agency personnel (civilians, military, military reservists, contractors, and defense contractors) complete intelligence oversight (IO) training annually.

(U//~~SI//NF~~) In addition, to qualify for the [redacted] credential and comply with the requirements of the BR Order, personnel must have completed specific training courses within the last 12 months. All courses are developed by NSA's ADET in conjunction with the OGC, mission subject matter experts and mission compliance professionals.

- (U//~~FOUO~~) **OWSC1000**, NSA/CSS Intelligence Oversight Training, the Agency's core IO course, is provided to the workforce to maintain a high degree of sensitivity to and understanding of intelligence laws, regulations, and policies associated with the protection of USP privacy rights during mission operations. Personnel are familiarized with the major tenets of the four core IO documents: Executive Order (EO) 12333, as amended; Department of Defense (DoD) Regulation 5240.1-R; Directive Type Memorandum (DTM) 08-052; and, NSA/CSSSP Policy J-23. OVSC1000 is web based and includes knowledge checks for proficiency.<sup>15</sup>
- (U//~~FOUO~~) **OVSC1100**, Overview of Signals Intelligence Authorities, the core SIGINT IO course, provides an introduction to various legal authorities that NSA uses to conduct its operations. Upon completion, personnel should be able to identify applicable surveillance authorities at a high level, defend the basic provisions of the authorities, and identify situations and circumstances requiring additional authority. OVSC1100 is web based and includes knowledge checks for proficiency. All personnel in the U.S. SIGINT System (USSS) working under the NSA Director's SIGINT authority with access to raw SIGINT are required to complete OVSC1100 every 12 months.
- (U//~~FOUO~~) **OVSC1800 (Analytic)** and **OVSC1806 (Technical)**, Legal Compliance and Minimization Procedures, advanced SIGINT IO course that explains policies, procedures, and responsibilities within mission and functions of the USSS to enable the protection of USP and foreign partner privacy rights. Upon successful completion, NSA analysts within mission requirements to access raw SIGINT databases will have met the additional training requirement imposed by SID. OVSC1800 and OVSC1806 are web based and include competency exams [redacted]

(b)(3) P.L. 86-36

[redacted] Personnel who do not pass the test after Q attempts must complete remedial training. All personnel in the USSS working under the NSA Director's SIGINT authority with access to raw SIGINT are required to complete OVSC1800 or OVSC1806 every 12 months.

<sup>15</sup> (U//~~FOUO~~) E.O. 12333, *United States Intelligence Activities*; DoD Regulation 5240.1-R, *Procedures Governing the Activities of DoD Intelligence Components That Affect U.S. Persons*; DTM-08-052, *DoD Guidance for Reporting Questionable Intelligence Activities and Significant or Highly Sensitive Matters*.

~~TOP SECRET//SI//NOFORN~~

ST-14-0002

- (U//FOUO) OVSCI205 (Analytic) and OVSCI206 (Technical), Special Training on BR FISA, advanced IO courses that present legal policies surrounding the FISC Orders and RAS Standard pertaining to specific CT focused programs. OVSCI205 and OVSCI206 are web based and include competency exams with a minimum passing score of 90 percent for OVSCI205 and 89 percent for OVSCI206, a higher proficiency threshold than other courses because BR FISA data has a greater probability of containing USP information. Personnel who do not pass the test after one attempt must complete remedial training. All personnel with access to the BR FISA program are required to complete OVSCI205 or OVSCI206 every 12 months.

(U//FOUO) **DoJ NSD review of training material** As the BR Order requires, NSA's OGC provides DoJ NSD copies of the material (e.g., OVSCI205 and OVSCI206 training courses) used to train NSA personnel on the authority. OGC most recently provided DoJ NSD copies of revisions to the training materials in February 2014. NSA had revised the training materials because of the 17 January 2014 program changes, which included the two-loop limitation and FISC RAS-approval process.

#### (U) Access requirements for technical personnel to BR repositories

(U//FOUO) The BR Order states that appropriately trained and authorized technical personnel may access the BR metadata to perform those processes needed to make the data usable for intelligence analysis. The following describes the repositories and systems and the access requirements for technical personnel.

(b)(1)  
 (b)(3)-P.L. 86-36  
 (b)(3)-50 USC 3024(i)

- (U//SI//NF) [REDACTED]

<sup>16</sup>(U//FOUO) Backup tapes are securely stored in a locked cabinet inside a restricted access room at a secure [REDACTED] facility and are only accessible by designated [REDACTED] personnel.

~~TOP SECRET//SI//NOFORN~~

TOP SECRET//SI//NOFORN

ST-14-0002

- (TS/NSMMF) [REDACTED]

(b)(16)

(b)(3)-P.L. 86-36

(b)(3)-50 USC 3024(i))

- [REDACTED]

- (U//FOUO) NSA's Corporate Infrastructure Technical personnel responsible for maintaining NSA's underlying corporate infrastructure and transmission of BR metadata to NSA (e.g., corporate [REDACTED] personnel and SharePoint system administrators) are not required to receive special training regarding the BR program.

(b)(3)-P.L. 86-36

**(U) Access requirements for analysts to query BR repositories**

(TS/NSMMF) To query the [REDACTED] database using [REDACTED], analysts, including DIAAs, must be listed on the [REDACTED] User Group in [REDACTED].

The process to be added to the user group was discussed in the [REDACTED]

When analysts log into [REDACTED] using their public key infrastructure

password, [REDACTED] verifies that the analysts are listed on the [REDACTED]

and they have the [REDACTED]

If all three requirements are met, the analyst is added to the [REDACTED] mode in [REDACTED] and query BR [REDACTED] had the ability to run queries on [REDACTED]

(b)(1)  
(b)(3)-P.L. 86-36

(U//FOUO) Table 14 summarizes the provisions of BR Order 113-11588 for access and training and the controls implemented by NSA to maintain compliance.

(b)(3)-P.L. 86-36

<sup>17</sup> (U//FOUO) [REDACTED] TD technical personnel system accesses to [REDACTED] were terminated.

<sup>18</sup> (U//FOUO) PKI is used to authenticate users on NSA networks. PKI binds public keys with users of a digital certificate authority. [REDACTED]

TOP SECRET//SI//NOFORN

~~TOP SECRET//SI//NOFORN~~

ST-14-0002

(b)(1)

(b)(3)-P.L. 86-36

## (U) Table 14. Access and Training Provisions and Controls

~~(TS//SI//NF)~~

| Provision  | Control  |
|--|--|
| (U) Access to BR metadata shall be restricted to authorized personnel who have received appropriate and adequate training.<br><br>(b)(3)-P.L. 86-36  | (TS//SI//NF) All personnel with access to BR metadata must be approved for the [ ] credential. All personnel with access to the BMD repositories must have the [ ] credential. All personnel who query the BR metadata in the BMD repositories must have the [ ] credential and be on the [ ] User Group in [ ]. All personnel with the [ ] credential must complete appropriate and adequate training verified and monitored by SV. |
| (U) Appropriately trained and authorized technical personnel may access the BR metadata to perform those processes needed to make it usable for intelligence analysis.   | (TS//SI//NF) Technical personnel with access to the BR metadata must have the [ ] credential and must have completed appropriate and adequate training verified and monitored by SV.   |
| (U) Technical personnel responsible for NSA's underlying corporate infrastructure and the transmission of the BR metadata from the specified persons to NSA will not receive special training regarding the authority granted herein.                                  | (U) Technical personnel responsible for NSA's underlying corporate infrastructure do not receive special training regarding the BR program.<br><br>(b)(1)<br>(b)(3)-P.L. 86-36   |
| (U) NSA's OGC and ODOC will further ensure that all NSA personnel who receive query results in any form first receive appropriate and adequate training and guidance regarding the procedures and restrictions for the handling and dissemination of such information. | (TS//SI//NF) Before an analyst sends BR-unique query results containing USP information to another individual, the analyst must confirm that the recipient has the [ ] credential.* An individual with the [ ] credential must complete and remain current on required training, which includes training and guidance on handling and disseminating such data.   |
| (U) NSA will maintain records of all such training.  | (U//FOUO) NSA's ADET Enterprise Learning Management database is NSA's SSR for maintaining training completion records.   |
| (U) OGC will provide DoJ NSD with copies of all formal briefing and/or training materials (including all revisions) used to brief/train NSA personnel concerning this authority.   | (U//FOUO) NSA's OGC provides BR FISA training material to DoJ NSD for review before modifying material in the OVSC1205 and OVSC1206 training courses.  |
| *(C//REL TO USA, FVEY)   |  |
|  | (TS//SI//NF)   |

## (U) Querying

(b)(3)-P.L. 86-36

## (U) Provisions of BR Order 13-158

~~(TS//SI//NF)~~ NSA may access BR metadata for purposes of obtaining foreign intelligence information only through queries of the BR metadata to obtain contact~~TOP SECRET//SI//NOFORN~~

chainning information usings selection terms approved seeds.<sup>19</sup> A seed is a selection term approved for querying BR metadata. All selection terms to be used as seeds with which to query the BR metadata must first be approved by the S214 Chief or Deputy Chief or one of the twenty specially authorized HMCs in the SID Analysis and Production Directorate.<sup>20</sup> Approval shall be given only if the designated approving official has determined that based on the factual and practical considerations of everyday life on which he is a sensible and prudent person, after there are facts giving rise to a RAS that the selection term to be queried is:

(hereafter the Foreign Powers). If the selection term is reasonably believed to be used by a USP, the NSA's OGC must first determine that the USP is not regarded as:

(b)(1) P.L. 86-36

(b)(3)-50 USC 3024(1)

solely on the basis of activities that are protected by the First Amendment to the Constitution.<sup>21</sup> RAS approvals shall be effective for 80 days or for any selection term reasonably believed to be used by a USP and one year for all other selection terms.

(U//FOUO) Furthermore, queries of the BR metadata using RAS approved selection terms may occur directly by an NSA analyst querying through the autoplated query process.<sup>22</sup> Contact chaining queries of BR metadata will begin with a RAS approved seed, and will return only that metadata within three "hops" of the seed.<sup>23</sup>

<sup>19</sup> (U//FOUO) The term "selection terms" includes but is not limited to "identifiers." The term "identifiers" means a telephone number, as that term is commonly understood and used:

<sup>20</sup> (TS//SI//NF) Selection terms that are the subject of electronic surveillance authorized by the FISC based on the FISC's finding of probable cause to believe that they are used by:

including those used by USPs, may be deemed approved for querying for the period of FISC-authorized electronic surveillance without review and approval by a designated approving official. On 26 February 2014, NSA began sending selection terms to the FISC for RAS approval to comply with the President's directive of 17 January 2014. On 28 February 2014, the FISC approved RAS for the first two selection terms under this new process.

<sup>21</sup> (U) The First Amendment to the U.S. Constitution prohibits making any law abridging the freedom of speech, infringing on the freedom of the press, interfering with the right to peaceably assemble, or prohibiting the petitioning for a government redress of grievances. (The BR Order no longer requires that NSA's OGC perform a First Amendment review of selection terms used by USPs for non-emergency RAS requests; the FISC performs those reviews. This change was made following the President's directive on 17 January 2014, which requires that NSA submit selection terms to the FISC for RAS approval.)

<sup>22</sup> (TS//SI//NF) The autoplated query process was initially approved by the FISC in the 7 November 2012 Order that amended docket number BR 12-178. Although approved, NSA never implemented and is no longer authorized to use the autoplated query process since it withdrew its request to do so in the renewal applications and declarations that support the BR Orders approved by the FISC (beginning with BR Order 14-67, dated 28 March 2014).

<sup>23</sup> (U//FOUO) The first hop from a seed returns results including all selection terms (and their associated metadata) with a contact and/or connection with the seed. The second hop returns results that include all selection terms (and their associated metadata) with a contact and/or connection with a selection term revealed by the first hop. The third hop returns results that include all selection terms (and their associated metadata) with a contact and/or connection with a selection term revealed by the second hop. On 29 January 2014, NSA's software system controls were modified to limit the number of hops from seed selection terms to two to comply with the President's directive of 17 January 2014.

~~-TOP SECRET//SI//NOFORN-~~

ST-14-0002

Appropriately trained and authorized technical personnel may query BR metadata using selection terms that have not been RAS approved to perform processes needed to make the BR metadata available for intelligence analysis and may analyze the results of those queries with other authorized personnel responsible for such purposes. However, the results of such queries may not be used for intelligence analysis purposes. NSA must ensure through adequate and appropriate technical and management controls that queries of BR metadata for intelligence analysis purposes will be initiated using only selection terms that have been RAS approved.

**(U) Presidential directives affecting querying controls in 2014**

(U) On 17 January 2014 and 27 March 2014, the President of the United States directed that NSA implement the following changes to the BR FISA program:

1. (U//FOUO) Submit selection terms to the FSSC for RAS approval. Before 17 January 2014, selection terms were RAS approved by the S2I4 Chief or Deputy Chief or one of the twenty specially authorized HMCs as the BR Order required, and OGC performed First Amendment reviews of selection terms associated with U.S. persons.
2. (U//FOUO) Restrict contact chaining to two hops from seed selection terms. Before 17 January 2014, appropriately trained and authorized NSA analysts were authorized to query up to three hops; however, NSA guidance restricted those analysts to query BR FISA repositories two hops from seed selection terms and one additional hop (the two hops of nested selection terms) with S2 division management approval.
3. (U//FOUO) Store BR metadata in provider controlled repositories and not in NSA repositories. Once implemented, NSA will submit FSSC approved RAS selection terms to providers for them to query their repositories. Providers will provide to NSA only the results of those queries.

(U//FOUO) NSA implemented the first two directives by February 2014. The third directive, storing BR metadata in provider repositories and obtaining only the query results from providers, will require passage of a new statute for the protection of business records, which has not been enacted when this report was issued.

(U//FOUO) The remainder of this section documents the control framework in place for querying BR metadata in 2013, including the changes implemented by the President's directives in 2014.

**(U) Determining seed selection terms for requesting RAS approval**

(U//FOUO) Analysts working CT missions focus on lead selection terms which can be derived from multiple sources.

(b)(3)-P.L. 86-36

Analysts apply a wide range of tradecraft in determining which selection terms to pursue RAS approval.

~~-TOP SECRET//SI//NOFORN-~~

(b)(3)-P.L. 86-36

(U//~~FOUO~~) Analysts making determinations whether selection terms are eligible to be used as seeds under the BR FISA authority must consider all the facts they know or reasonably can know before submitting requests for RAS approval. Looking at the totality of the circumstances, analysts evaluate whether there is a RAS that the selection term is associated with persons associated with one of the terrorist organizations in the BR Order. The level of proof demanded by the RAS standard is less than a preponderance of the evidence or probable cause.

(b)(3)-P.L. 86-36

(U//~~FOUO~~) Nonetheless, the RAS standard requires more than a mere hunch or uninformed guesswork. Analysts must have an "articulable reason", supported by at least one source, for suspecting that the person using the selection term is associated with one of the terrorist organizations in the BR Order. Sources used to justify RAS requests include but are not limited to,

<sup>24</sup> The RAS standard is the same for selection terms associated with USPs and foreign persons.

(b)(3)-P.L. 86-36

(TS//SI//NF) Analysts electronically submit RAS requests in [REDACTED]-NSA's RAS selection term management system. [REDACTED] has required fields for analysts to enter justifications for RAS requests, user nationalities, and user ties to at least one of the terrorist organizations in the BR Order. Analysts save the supporting documentation for RAS requests in [REDACTED] for review by designated officials. As authorized by the BR Order, if selection terms are subject to ongoing HISC-authorized electronic surveillance [REDACTED] based on a finding of probable cause that the selection term is used to be used by persons associated with one of the identified foreign powers, NSA may use the selection terms to query the BR metadata without obtaining RAS because probable cause, a higher standard, has already been met. In these cases, entries are submitted through [REDACTED] along with supporting documentation and HMC and possible OGC review (if a selection term is associated with a USP) would also be required. According to (b)(3)-P.L. 86-36 a majority of the selection terms submitted for RAS approval are derived from [REDACTED]

(b)(1)

(b)(3)-P.L. 86-36

(b)(3)-50 UISC 3024(i)

(TS//SI//NF) Maintaining the [REDACTED] list in [REDACTED]

(TS//SI//NF) [REDACTED]

<sup>24</sup> (U//~~FOUO~~) If RAS requests are based in part or in whole on NSA SIGINT, NSA performs a purge verification check for the selection term when the request is submitted to ensure that the selection term had not been submitted for on-demand, retroactive, or reactionary removal of data from NSA SIGINT system repositories. The "purge verification" field must be filled out when creating a RAS request and must be conducted no more than 24 hours before submission.

TOP SECRET//SI//NOFORN

ST-14-0002

(b)(1)  
 (b)(3)-P.L. 86-36  
 (b)(3)-50 USC 3024(i)



(TS//SI//NF) RAS can be met only on selection terms associated with the terrorist organizations listed in [REDACTED]. Those would include organization listed in the FISC-approved BR Order or based on IC reporting and determined by NSA's OGC and SV as [REDACTED] a terrorist organization in the FISC-approved BR Order.<sup>25</sup>

(b)(3)-P.L. 86-36

Only individuals assigned the [REDACTED] role can maintain the terrorist organization list in [REDACTED]. NSA personnel were assigned this role [REDACTED] (b)(1)

(TS//SI//NF) [REDACTED] which NSA implemented in June 2010, provides the system control framework for nominating, justifying, reviewing, approving, and disapproving RAS for selection terms. [REDACTED] has built-in safeguards to ensure that RAS approved selection terms comply with requirements of the BR Order (e.g., required RAS approvals documented only approved terrorist organizations used for RAS, maximum time limit not exceeded for RAS approvals). [REDACTED] also serves as the authoritative source for RAS approved selection terms and exports the selection terms to other systems in the BR control framework.

(b)(3)-P.L. 86-36

#### (U) RAS approval process-2013

(U//FOUO) In 2013, the RAS approval process included certain mechanisms NSA used to determine whether selection terms were associated with one of the terrorist organizations in [REDACTED] before BR authorized analysts could use the selection terms as seeds to query BR metadata. Consistent with the BR Order, all selection terms used as seeds for querying BR metadata were first approved by the S2I4 Chief

(b)(1)

(b)(3)-P.L. 86-36

<sup>25</sup> (TS//SI//NF) In May 2012, DoJ NSD stated that it was generally acceptable for NSA's OGC to determine, based on its own analysis, whether selection terms were associated with one of the terrorist organizations in [REDACTED].

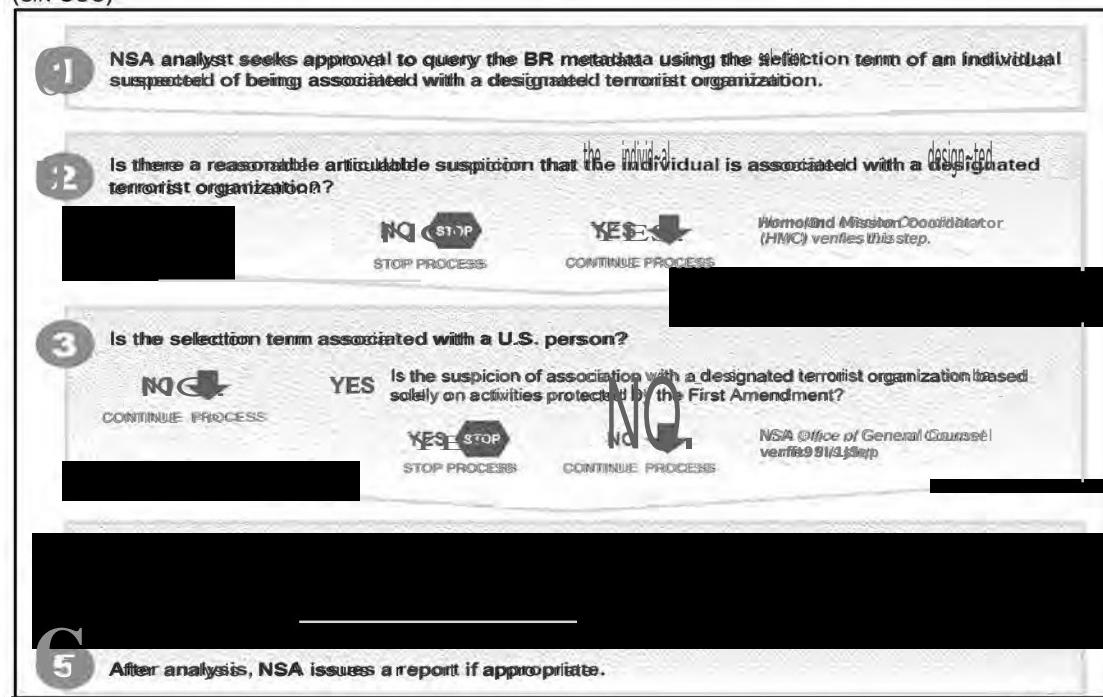
In addition, with the condition of RAS being met, NSA can include [REDACTED]  
 DoJ NSD further stated that OGC must revisit those determinations every six months [REDACTED]

TOP SECRET//SI//NOFORN

or Deputy Chief or one of the 20 specially authorized HMCs. If selection terms were reasonably believed to be used by USRs, NSA's OGC determined whether the USPs were regarded as associated with one of the terrorist organizations named in the BR Order solely on the basis of activities protected by the First Amendment. Figure 4 illustrates the RAS approval process in place during 2013.

**(U) Figure 4. RAS Approvals Needed Before Querying BR Metadata in 2013**

(U//FOUO)



(U//FOUO)

(U//FOUO) Table 15 summarizes the RAS selection terms approved in 2013.

**(U) Table 15. 2013 RAS Approvals** (b)(3)-P.L. 86-366  
(b)(3)-50 USC 3024(i)

| (TS//SI//NF) |  |
|--------------|--|
| Approved     | Approved   |
| *            | (U//FOUO) Data includes RAS selection terms that were approved more than once in 2013. |

\* (U//FOUO) Data only includes unique selection terms approved during 2013; it excludes multiple RAS approvals for the same selection terms in 2013.

(TS//SI//NF)

**(U) HMC review process-2013**

(U//FOUO) After RAS approval requests are submitted in [REDACTED] automatic e-mail notifications are sent to HMCs alerting them that requests are available for review. Depending on the ranking assigned to RAS approval requests in [REDACTED] reminder emails are sent after [REDACTED] for emergency requests, [REDACTED]

TOP SECRET//SI//NOFORN

ST-14-0002

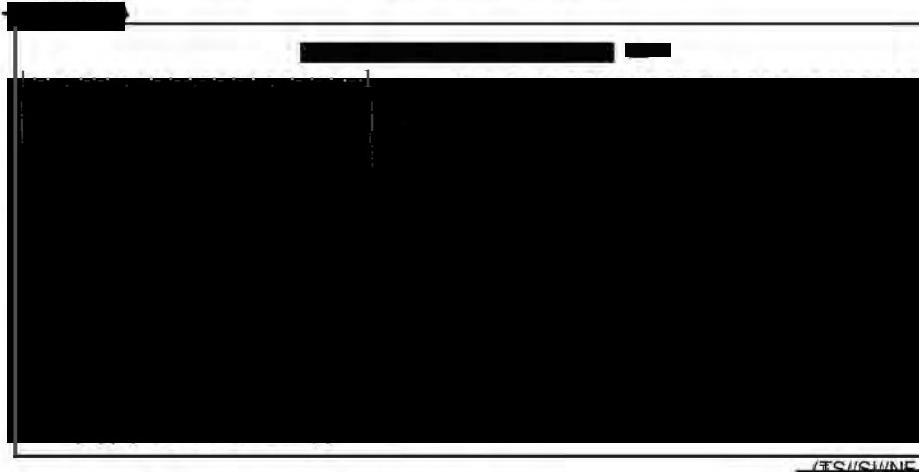
requests, [ ] for priority requests, and [ ] for routine requests. HMCs verify that:

- (U//FOUO) Justifications sufficiently and accurately document the series to the selection team submitted for RAS approval;
- (U//FOUO) Justifications clearly support series to one of the terrorist organizations listed in [ ]
- (U//FOUO) RAS requests are supported by credible source documentation;
- (U//FOUO) Source documentation is current and has not been superseded by other intelligence; RAS requests contain time restrictions, if selection terms are or were associated with users so to only as specific and limited time, and
- (U//FOUO) If SIGINT is used as justification for RAS approval requests, analysts performed purge verifications when requests are submitted.

(U//FOUO) If HMCs determine that the documentation requirements have not been met and the RAS standard has not been met, analysts are notified of deficiencies and asked to provide additional information. HMCs denote denied RAS requests as "Pending" until adequately documented in [ ]. If the documentation requirements are met and the RAS standard has been satisfied, HMCs change the status of requests from "Pending" to "Approved" in [ ].<sup>26</sup>

Change logs in [ ] document status changes and edits of the original RAS approval requests by analysts and designated approvers. For oversight purposes, change log histories cannot be edited. [ ] system controls require that OGC approve selection terms used by USPs before completing the RAS approval process. Figure 5 illustrates the RAS standard.

(U//FOUO) Figure 5. RAS Standard



-(TS//SI//NF)-

(b)(3)-P.L. 86636

<sup>26</sup> (U//FOUO) Some BR trained and authorized analysts can approve RAS requests and query BR metadata. However, [ ] system controls prevent persons from submitting and approving their own RAS requests.

TOP SECRET//SI//NOFORN

## (U) OGC First Amendment review of seed selection terms associated with USPs-20033

(U//FOUO) NSA is prohibited from establishing RAS on a USP selection term based solely on activities protected by the First Amendment. In 2013, RAS requests containing selection terms associated with USPs were forwarded to the NSA OGC for a First Amendment review. [REDACTED] sent automated email notifications to designated OGC attorneys until First Amendment reviews completed. OGC reviewed the RAS requests and source documentation, as well as the RAS decisions made by HMCs, and determined whether NSA intended to target individuals based solely on activities protected by the First Amendment. If there were indications that RAS requests were based solely on such activities, OGC would deny the RAS request (denoted as "Disapproved" in [REDACTED]). Once OGC has approved RAS requests in [REDACTED], the selection terms are authorized for use as seeds for querying.

However, a series of system updates must be completed before analysts can query BR metadata using newly approved seed selection terms. [REDACTED]

(b)(3)-P.L. 86-36

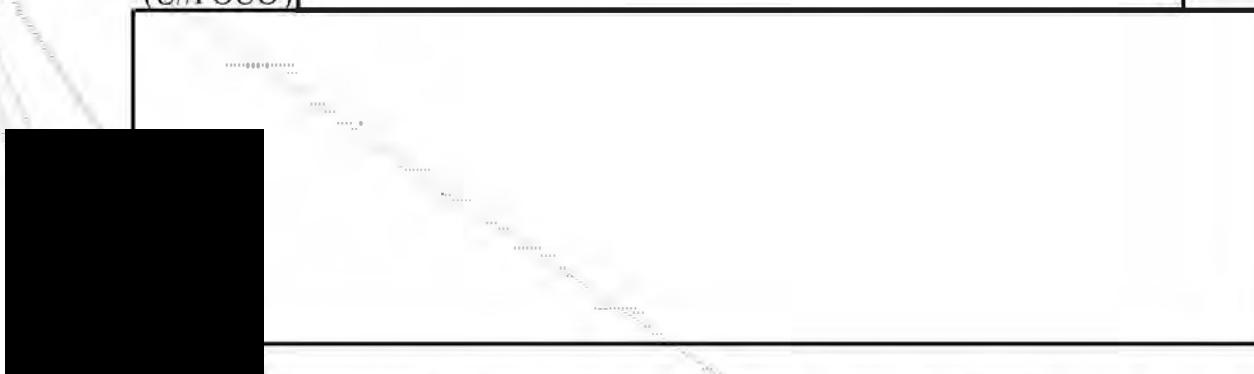
(b)(1)r

(b)(3)-P.L. 86-36

## (U) Controls for querying BR metadata using only RAS approved seed selection terms within the authorized number of hops

(U//FOUO) [REDACTED] tracks the status of selection terms and for an "Approved" status the expiration of the RAS approval. The BR Order specifies that RAS approvals shall be effective for 180 days for selection terms reasonably believed to be used by USPs and one year for all other selection terms. However, NSA, out of an abundance of caution, used a more restrictive RAS expiration policy in 2013: 90 days for selection terms used by USPs and 180 days for selection terms used by foreign persons.<sup>27</sup> [REDACTED] is configured to automatically change the status of RAS selection terms from "Approved" to "Expired" when expiration dates NSA set are exceeded. terms from "Approved" to "Expired" when expiration dates NSA are exceeded.

(U//FOUO) [REDACTED]



(U//FOUO) [REDACTED] is the graphical user interface that analysts use to query data in [REDACTED] including BR metadata. When launching [REDACTED] analysts with

<sup>27</sup> (U//FOUO) [REDACTED] was reconfigured so that selection terms used by USPs expired in 173 days and 358 for all others. NSA made this change to avoid burdening the FISC, which began approving RAS for selection terms as the President had directed, with more frequent reauthorizations than the BR Order requires.

~~-TOP SECRET//SI//NOFORN~~

ST-14-0002

appropriate credentials have the option to include BR metadata in their queries. If analysts select the [redacted]

(b)(1) (b)(3)-P.L. 86-36 [redacted]

~~(TS//SI//NF)~~ When in the [redacted] mode of [redacted] analysts may only use a RAS approved selection term to query BR metadata. The term used to initiate a query of BR metadata is referred to as a seed because it is used to produce a "chain" of metadata contacts, known as contact chaining. When analysts submit seed selection terms for querying using [redacted] another part of [redacted] middleware called the Emphatic Access Restriction (EAR) checks whether the selection terms appear as "Approved" in the [redacted] tables.<sup>28</sup> The EAR, through internal software system controls, ensures that contact chaining is restricted to seeds that are RAS approved by preventing non RAS approved selection terms from being used as seeds for conducting full chaining analysis of BR metadata in [redacted] (e.g., expired, decommissioned, disapproved selection terms, terms that have never been entered into [redacted]). If selection terms submitted by analysts for querying of BR metadata appears as "Approved" in the [redacted] tables, the EAR allows queries to perform. The EAR prevents queries from performing when the selection terms do not appear as "Approved."

~~(U//FOUO)~~ In 2013, the EAR software system controls also restricted the number of hops to three from the seed for contact chaining, as the BR Order authorized.<sup>29</sup> However, if analysts, after receiving the first two hops results awarded to perform contact chaining out to a third hop from the seed selection term, SID policy required that they first obtain S2 division management approval. NSA relied on analysts to comply with SID policy—no system control was implemented to prevent analysts from querying out to three hops without S2 division management approval.

~~(U//FOUO)~~ To understand how contact chaining was performed and the system controls implemented by the EAR to only allow querying using RAS approved seeds and within three hops of the seed selection term in 2013, it is helpful to review an example.

(b)(1) (b)(3)-P.L. 86-36

~~(S//REL TO USA, FVEY)~~ Seed selection term A reasonably believed to be used by a foreign person [redacted] was RAS approved by an HMC. No First Amendment review was required because selection term A (the seed) was not used by a U.S. person. The analyst entered selection term A in to [redacted] to perform contact chaining analysis one hop from the seed. The EAR automatically checked the [redacted] tables to determine whether

(b)(3)-P.L. 86-36

<sup>28</sup> ~~(TS//SI//NF)~~ NSA implemented the EAR [redacted]. Before then, NSA relied on analytic due diligence to query [redacted] (BR metadata). With only RAS approved selection terms<sup>C</sup> After [redacted] release in June 2010, the EAR was reconfigured to use data from [redacted] to prevent queries in [redacted] using selection terms that were not RAS approved, including USP selection terms that OGC had not reviewed.

<sup>29</sup> ~~(TS//SI//NF)~~ On 29 January 2014, NSA modified the EAR software system controls to reduce the number of hops from the seed to two to comply with the President's directive of 17 January 2014.

~~-TOP SECRET//SI//NOFORN~~

TOP SECRET//SI//NOFORN

(b)(3)-P.L.86-36

ST-14-0002

(b)(1) selection term A was RAS approved. Because it showed as RAS approved the EAR allowed the query of BR metadata in [REDACTED]. First hop queries returned all selection terms available in the BR repository (and associated metadata) that had a contact or connection with the seed [REDACTED]

(b)(1)  
(b)(3)-P.L. 86-36  
(b)(3)-18 USC 708  
(b)(3)-50 USC 3024(i)

[REDACTED] If the analyst tried to query beyond the third hop or query using a selection term that had not been RAS approved the EAR would have prevented the action.

#### (U) EAR bypass

(S//SI//NF) Because it can take [REDACTED] for system updates to complete before a RAS approved selection term can be used for querying BR metadata, an EAR bypass was implemented for emergency situations. If an analyst, with a RAS approved seed selection term and S2I4 management approval, determines that immediate querying of BR metadata using the RAS approved selection term is necessary to obtain time-sensitive results to respond to an emergency, S2I4 informs designated OGC, SV, and ODOC personnel of its intention to bypass the EAR software system controls. After this notification S2I4 management contacts the [REDACTED] team requesting that the designated analyst be temporarily added to the [REDACTED] user group in [REDACTED]. This allows the analyst to select the bypass option in [REDACTED] thereby bypassing the EAR software system controls for hop restrictions and checks off RAS selection terms against the [REDACTED] tables. Analysts, with manual checks by direct on-site supervisor oversight, ensure that queries performed in the bypass mode do not exceed three hops (before 17 January 2014) or two hops (on and after 17 January 2014). The [REDACTED] team is notified when the analyst should be removed from the [REDACTED] user group in [REDACTED] immediately following NSA's response to an emergency situation or after formal system updates have completed to allow querying using the RAS approved selection terms. No NSA personnel were included in the [REDACTED] user group [REDACTED]

#### (U) Querying by trained and authorized technical personnel for testing purposes only

(S//SI//NF) The BR Order allows authorized NSA technical personnel to access the BR metadata, including through queries, to make it usable for intelligence analysis. This includes performing [REDACTED]

and maintaining records to demonstrate compliance with the BR Order. However, technical personnel do not share the results of these queries with analysts. Tests of BRM [REDACTED] as the BR Order allows. Only a limited number of technical personnel, who appear in the [REDACTED]

TOP SECRET//SI//NOFORN

(b)(3)-P.L.86-36

~~TOP SECRET//SI//NOFORN~~

(b)(1)

(b)(3)-P.L. 86-36

ST-14-0002

(b)(3)-P.L. 86-36 user group in [REDACTED] can query BR metadata using non RAS approved selection terms in operational databases. The [REDACTED] user group is used only by technical personnel. SV audits all queries performed using query tools by technical and mission personnel to ensure compliance with the BR Order. [REDACTED] authorized NSA technical personnel were in the [REDACTED] user group [REDACTED]

**(U) RAS approval process-2014**

(TS//SI//NF) On 17 January 2014, the President directed that NSA implement changes in how it operates the BR FISA program: NSA must submit selection terms to the FISC for RAS approval and limit contact chaining to two hops from the seed selection terms. Before 17 January 2014, RAS selection terms were approved by the S2I4 Chief or Deputy Chief or one of the twenty authorized HMCs, as the BR Order required, and contact chaining was allowed out to three hops:

(b)(1)

(b)(3)-P.L. 86-36

[REDACTED] - 1 - As an added measure, on 23 January 2014, all RAS selection terms in an "Approved" status were changed to "Revalidate" in [REDACTED] (b)(3)-P.L. 86-36

(U//FOUO) In the weeks following the President's directives, through a motion to amend BR Order 14-01 the FISC approved on 5 February 2014, the following:

(U) The government may request, by motion and on a case-by-case basis, permission from the Court for NSA to use specific selection terms that satisfy the RAS standard as "seeds" to query the BR metadata to obtain contact chaining information, within two hops of an approved "seed," for purposes of obtaining foreign intelligence information. In addition, the Director or Acting Director of NSA may authorize the emergency querying of the BR metadata with a selection term for purposes of obtaining foreign intelligence information within two hops of a "seed," if: (1) the Director or Acting Director of NSA reasonably determines that an emergency situation exists with respect to the conduct of such querying before an order authorizing such use of a selection term can with due diligence be obtained; and (2) the Director or Acting Director of NSA reasonably determines that the RAS standard has been met with respect to the selection term. In any case in which this emergency authority is exercised, the government shall make a motion in accordance with this amendment to the BR Primary Order to the Court as soon as practicable, but not later than seven days after the Director or Acting Director of NSA authorizes such query.

(U//FOUO) In response to these new requirements, the NSA BR control framework changed:

- (U//FOUO) RAS approvals submitted to the FISC NSA no longer approves RAS for selection terms, except in emergency situations. HMCs or the S2I4 Chief or Deputy Chief previously approved RAS. They now perform

(b)(3)-P.L. 86-36

only first level reviews to determine whether RAS requests are adequately documented and supported by creditable source documentation in [redacted]

[redacted] Analysts follow the same preliminary procedures before for determining whether selection terms are used by persons who are reasonably believed to be associated with one of the terrorist organizations listed in the BR Order and for documenting RAS requests in [redacted]. After reviewing the supporting documentation, HMCs send RAS requests back to analysts to make additional changes (as needed), deny RAS requests, or formally endorse them. Only RAS requests endorsed by HMCs are submitted in [redacted] to OGC for second level review (regardless of whether selection terms are used by USPs or foreign persons).

(b)(3)-P.L. 86-36

(U//FOUO) OGC no longer officially performs First Amendment review of selection terms used by USPs for non-emergency RAS requests; the FISC performs those reviews. OGC now performs second level reviews for RAS requests, source documentation and endorsement decisions by HMCs to provide greater assurance that the FISC will not reject RAS requests because of insufficient documentation or First Amendment concerns (for selection terms used by USPs). OGC reviews HMC endorsements during RAS verification meetings at which HMCs present evidence supporting the RAS justifications for review by SV, OGC, and the S2 Declarant (usually the S214 Chief or Deputy Chief) who signs the eventual motion seeking FISC approval of the selection terms. This group (known as the "RAS verification panel"), chaired by SV, confirms that representations in RAS requests are accurate. If the RAS verification panel endorses the RAS requests, OGC submits them to DoJ NSD for review and submission to the FISC for approval. At each level of review by HMCs, OGC, the RAS verification panel, and DoJ NSD, all questions, concerns and requests for additional information must be satisfied before DoJ NSD submits the requests to the FISC.

(S//SI//NF) The FISC makes the final determination of whether the RAS standard has been met for each request and notifies DoJ NSD of its decision to approve or disapprove requests. After OGC has been notified by the DoJ NSD of the FISC decision, OGC enters the date of the decision, saves the supporting court documentation, and updates the disposition of RAS requests in [redacted] as "Approved" or "Disapproved."<sup>31</sup> FISC approvals are effective for 180 days for selection terms used by USPs and one year for all others. However, NSA established slightly more conservative expirations [redacted] 173 days for selection terms used by USPs and 358 days for all others. Figure 66 illustrates the non-emergency RAS approval process.

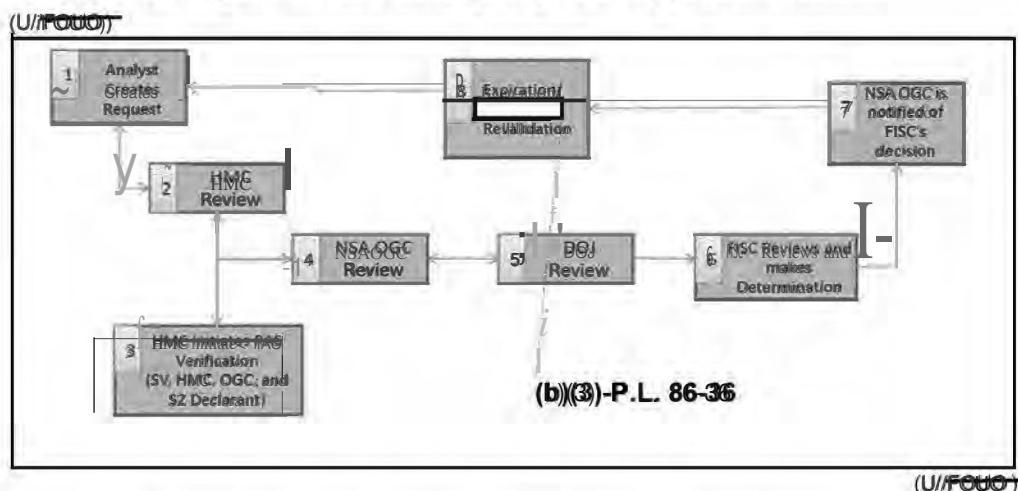
(b)(3)-P.L. 86-36

<sup>31</sup> (U//FOUO) [redacted] is the system of record for storing documents relating to NSA authorities, including BR Orders for the BR FISA authority.

~~TOP SECRET//SI//NOFORN~~

ST-14-0002

## (U) Figure 6. Non-Emergency RAS Approval Process



(b)(3)-P.L. 86-36

- (U//~~FOUO~~) **Emergency RAS approvals** Under the BR Order, the NSA Director (DIRNSA) or Acting DIRNSA can approve RAS for selection terms for querying BR metadata within two hops off the seed selection term only after the RAS standard has been met and only when responding to emergencies. When submitting a RAS request for emergency approval, analysts document the request and justification for emergency approval in [REDACTED]. An HMC performs a first-level review and requests additional information from the analysts (as needed) and denies or endorses the emergency RAS request. If the HMC endorses, the RAS verification panel is immediately convened to review the supporting documentation and justification for requesting emergency approval. If the RAS request contains a selection term used by a USP, OGC performs a First Amendment review to determine that the basis for seeking RAS is not solely based on activities protected by the First Amendment. If the RAS verification panel concurs with the HMC's endorsement and OGC concludes that there are no First Amendment concerns, the S2 Declarant, BR FISA Authority Lead, SV, and OGC will brief the DIRNSA or Acting DIRNSA, who determines whether an emergency situation exists, and the RAS standard has been met and the RAS determination is based solely on First Amendment protected activities.
- (U//~~FOUO~~) If the DIRNSA or Acting DIRNSA approves the emergency RAS request, OGC saves the approval documentation and changes the disposition of the RAS request to "Approved" in [REDACTED] and notifies DoJ NSD of the emergency RAS approval. If immediate querying is required, S2I4 coordinates adding the designated analyst to the [REDACTED] user group in [REDACTED] (see Querying Section for EAR Bypass procedures). Otherwise, the designated analysts must wait [REDACTED] for a series of system updates to complete before querying BR metadata using the emergency-approved selection term.

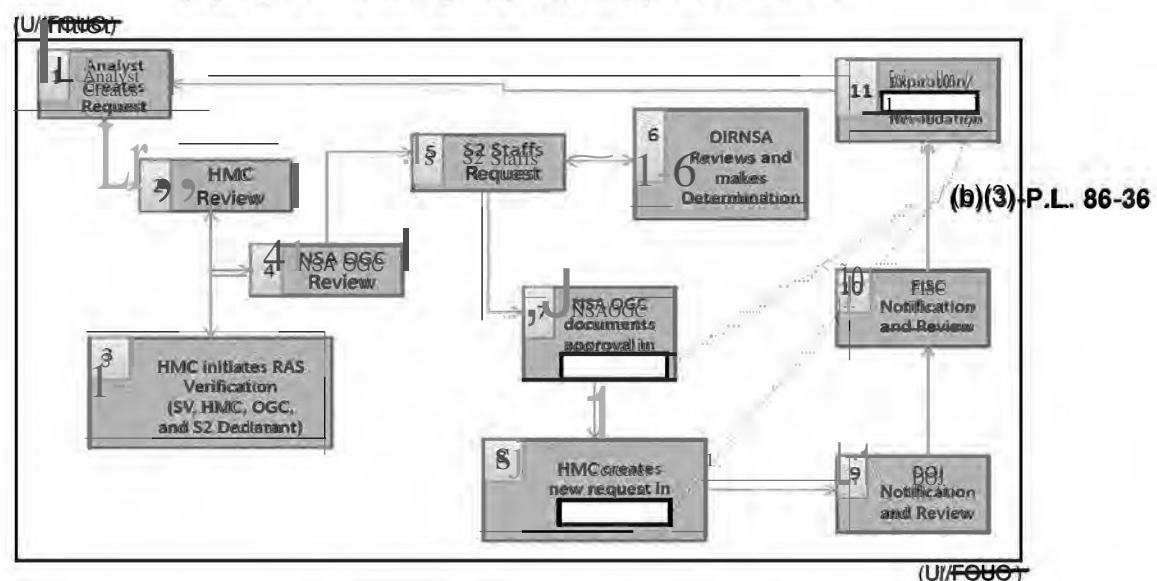
(U//~~FOUO~~) The BR Order requires that, within seven days of the emergency RAS approval, DoJ NSD file a motion with the FISC on behalf of NSA

~~TOP SECRET//SI//NOFORN~~

(b)(3)-P.L. 86-36

concerning the emergency authorization. If the FISC grants the motion, OGC enters the date the FISC approved the RAS query and records the supporting court documentation. If the FISC denies the motion, NSA will take remedial action, including actions the FISC has directed. Figure 7 illustrates the emergency RAS approval process.

(U) Figure 7. Emergency RAS Approval Process

(b)(1)  
(b)(3)-P.L. 86-36

(Q//REL TO USA, FVEY) [redacted] the DIRNSA approved the first and only selection term for emergency querying since receiving this new mandate from the FISC on 5 February 2014. A motion was filed with the FISC within several days of the DIRNSA's approval of the emergency RAS request. [redacted] the FISC approved RAS for this selection term.

- (U//FOUO) Two-hop restriction for contact chaining. On 29 January 2014, NSA modified the FARR software system controls to restrict contact chaining to two hops from seed selection terms as the President had directed. Before 17 January 2014, authorized NSA analysts could query BRRFSA repositories two hops from seed selection terms and one additional hop (the two hops from seed selection terms) with S2 division management approval.

(U) Table J6 summarizes the provisions of BR Order 13-158 for querying BR metadata and the controls NSA implemented to maintain compliance.

TOP SECRET//SI//NOFORN

ST-14-0002

## (U) Table 16. Querying Provisions and Controls

(U//FOUO)

| Provision   | Control   |
|---|---|
| (U//FOUO)<br>Seed selection terms must be approved by a designated approving official and also reviewed by OGC, if the selection term is used by a USP, before querying BR metadata for intelligence analysis purposes..  | In 2013, [ ] controls ensured that one of the 22 designated approving officials approved RAS for selection terms and, if used by USPs, OGC performed a First Amendment review. Selection terms were added to the RAS Approved List only after the required approvals were documented in [ ] |
| (U//FOUO)<br>Approvals shall be given only after the designated approving official has determined that there are facts giving rise to RAS that the selection term to be queried is associated with a Foreign Power.   | [ ] stores supporting documentation for justifying RAS; it also maintains the authoritative list of foreign powers.<br><br>(b)(3)-P.L. 86-36  |
| (U//FOUO)<br>NSA shall ensure, through adequate and appropriate technical and management controls, that queries of the BR metadata for intelligence analysis purposes will be initiated using only a selection term that has been RAS approved.   | EAR restricts contact chaining to only those seeds that are RAS approved by preventing all non RAS approved selection terms (e.g., expired, disapproved) from being used as seeds for conducting contact chaining.  |
| (U//FOUO)<br>RAS approvals must not exceed 180 days for selection terms reasonably believed to be used by a USP and 365 days for all other selection terms.   | [ ] automatically changes the status of RAS approved selection terms from "Approved" to "Expired" when expiration dates set by NSA are exceeded. In 2013, expiration dates were set for 90 days for selection terms associated with USPs and 808 days for all others. <sup>*</sup>          |
| (U//FOUO)<br>Results of contact chaining queries must not exceed three hops from seed selection terms.  | In 2013, the EAR limited the number of hops to three from the seed selection term for contact chaining. <sup>†</sup>  |
| (U//FOUO)<br>Technical personnel may query the BR metadata using selection terms that have not been RAS approved to perform processes needed to make it usable for intelligence analysis.   | SV reviews all query records for compliance with the BR Order.  |
| * (U//FOUO) On 26 February 2014, NSA began sending RAS requests to the FISC for approval to comply with the President's directive of 17 January 2014. On 28 February 2014, the FISC approved RAS for a selection term under this new process, and NSA began the process of manually entering into [ ] the dates that the FISC approved RAS for selection terms. [ ] was updated to require that FISC approval dates be inputted into it before adding selection terms to the RAS Approved List. |   |
| † (U//FOUO) The EAR relies on RAS approved selection terms to be accurately entered by authorized personnel manually into [ ]. In 2014, NSA discovered instances of RAS approved selection terms that were inaccurately entered into [ ] by authorized personnel. In response, NSA implemented a two-person review for accuracy of RAS approved selection terms manually entered into [ ].  |   |
| * (U//FOUO) [ ] the expiration dates in [ ] were changed to 173 days for selection terms used by USPs and 358 days for all others.  |   |
| § (U//FOUO) [ ] the EAR software system controls were modified to limit the number of hops from seed selection terms to two to comply with the President's directive from 17 January 2014.  |   |

(U//FOUO)

(b)(3)-P.L. 86-36

**(U) Sharing and Dissemination****(U) Provisions of BR Order 13-15B**

**(U//FOUO) Sharing** Results of intelligence analysis queries of BR metadata may be shared, before minimization, of intelligence analysis is among NSA Analysts subject to the requirement that all NSA personnel who receive query results in any form first receive appropriate and adequate training and guidance regarding the procedure for handling and disseminating such information.

**(U//FOUO) Dissemination** NSA shall apply the minimization and dissemination requirements and procedures of Section 7 of USS. Signals Intelligence Directive (USSID) SP0018 to any results from queries of the BR metadata, in any form, before the information is disseminated outside NSA in any form. In addition, before disseminating USP information outside NSA, the Director or Deputy Director or one of the officials listed in Section 7.3(c) of USSID SP0018 (i.e., Director of SID, Deputy Director of SID, Chief of Information Sharing Services (SIS), Deputy Chief of SIS, and the Senior Operations Officer of the National Security Operations Center) must determine that the information identifying the USP is related to CT information and it is necessary to understand the CT information or assess its importance ("CT nexus"). Approximately every 30 days, NSA shall file with the Counterintelligence, among many things, includes a statement of the number of instances since the preceding report in which NSA has shared, in any form, results from queries of the BR metadata that contain USP information in any form with anyone outside NSA.

(b)(3)-P.L. 86-36

**(U) Sharing BR-unique information with authorized NSA personnel**

**(TS//SI//NF)** NSA refers to "sharing" as providing query results internally to appropriately trained and authorized NSA personnel. Sharing restrictions in the BR Order only apply to BR-unique query results of a USP. "BR unique" is a term used by NSA that refers to contacts [REDACTED] within a chain solely derived from BR metadata [REDACTED] Oral or written depiction, manipulations, and summaries are also query results. Unless already included in a disseminated report, BR-unique query results containing USP information are only shared with individuals who have the [REDACTED] credential. BR stakeholders manually check [REDACTED] to confirm that recipients have [REDACTED] before sharing BR-unique USP information, in any form. BR stakeholders also ensure that documents or files containing BR-unique USP information are only stored in access-controlled, personal or shared network locations accessible only to BR-cleared personnel and that BR-unique results containing USP information displayed in the workplace are not visible to analysts who do not have [REDACTED].

(b)(1)

(b)(3)-P.L. 86-36

**(U//FOUO)**

~~TOP SECRET//SI//NOFORN~~

ST-14-0002

(b)(3)-P.L. 86-36

**(U) Disseminating BR unique information**

(U) Dissemination is the sharing of information outside NSA. The BR Order includes two provisions for disseminating information: the CT nexus requirement and the dissemination tracking requirement.

- (U//~~FOUO~~) **CT Nexus Requirement** The CT nexus requirement applies only to disseminations of BR query results containing USP information. The dissemination provisions of Section 7.3(c) of USSID SP0018 must be followed. If query results include USP information unique to BR metadata and the analyst needs to disseminate that information to an external customer, such as the FBI, then the CT nexus requirement must be met before disseminating information in any form. However, if query results contain only foreign person information, the CT nexus requirement does not apply when disseminating BR information. The remainder of this section focuses on disseminating USP information derived from BR unique metadata.

~~(TSM/SL/NM)~~ In accordance with USSID SP0018, if unminimized USP information is to be disseminated, one of the designated approval authorities must determine that the information is necessary to understand the foreign intelligence in the report before the information is released. This applies to all disseminations of unminimized USP information under all NSA authorities. The BR Order further requires that one of the approving authorities confirm that the information identifying USP also relates to CT information and is necessary to understand the CT information or assess its importance. SJS stated that most disseminations of USP information derived from BR metadata

(b)(1)

(b)(3)-P.L. 86-36

(b)(3)-50 USC 3024(i)

(U//~~FOUO~~) There are two categories of BR disseminations: Published disseminations [redacted]

[redacted] and other disseminations (e.g., oral briefings to recipients external to NSA, such as the FISC, who are not receiving the information as part of their lawful executive or legislative oversight function).

(b)(3)-P.L. 86-36

b (U//~~FOUO~~) [redacted] reports are used to disseminate SIGINT information that responds to special IC requirements [redacted]

[redacted] reports are disseminated in a limited distribution to customers empowered to act on the information and to additional customers who have an operational need-to-know (e.g., FBI, NCTC, Central Intelligence Agency (CIA), Office of the Director of National Intelligence (ODNI)).

~~TOP SECRET//SI//NOFORN~~

ST-14-0002

- o (U//~~FOUO~~) RFIs are requests by customer(s) (e.g., FBI) for information from NSA. RFIs are usually requests requiring general or specific responses.
- o (U//~~FOUO~~) [ ] are SIGINT reports that generally focus on one topic or event [ ]

(b)(3)-P.L. 86-36

variety of collection authorities to a wide audience. However, [ ] are not used to disseminate USP information unique to BR metadata [ ]

(b)(3)-P.L. 86-36

(U//~~FOUO~~) After one of the approving authorities listed in Section 7.3(c) of USSID SP0018 has approved the dissemination, if USP information unique to BR metadata is included in an [ ] it is usually combined with information from other collection authorities to provide a more complete intelligence summary. Otherwise, NSA masks the identities of USPs mentioned in [ ] (e.g., USP1), so that the [ ] can be distributed widely and sends separately an Identities Release Memorandum only to those parts of the IC that need to know the person's identity. Only these recipients within the IC who receive both the [ ] and Identities Release Memorandum can determine the USP identity, and this only after submitting formal justification requests that have been approved by one of the officials listed in Section 7.3(c) of USSID SP0018.

(U//~~FOUO~~) Dissemination of BR information occurs most often in [ ] reports. SJS stated that, even when NSA disseminates information using RFIs, corresponding [ ] reports follow to formally document the dissemination.<sup>32</sup> This allows the information requested by one IC customer, but important to other IC customers, to be released through a slightly wider, albeit highly controlled, distribution. Table 17 summarizes the BR reports disseminated in 2013.

(b)(3)-P.L. 86-36

<sup>32</sup> (U//~~FOUO~~) Masking is the process of using generic identifiers instead of USP names, titles, or contextual identifiers so that the person's identity is not revealed in written or oral disseminations.

<sup>33</sup> (U//~~FOUO~~) S214 confirmed that all RFIs containing BR unique information have been followed up with [ ] reports [ ]

~~TOP SECRET//SI//NOFORN~~

~~TOP SECRET//SI//NOFORN~~

ST-14-0002

(U) Table 17. BR Reports Disseminated in 2013 (b)(1)  
(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36

| (TS//SI//NF)   |  | RFIs | Other | Total |
|--|--|------|-------|-------|
| BR Reports Disseminated*   |  |      |       |       |
| Total Selection Terms Reported (Derived from BR  |  |      |       |       |
| Total BR Unique Selection Terms Reported†  |  |      |       |       |
| Total U.S. Contacts Reported†  |  |      |       |       |
| * There were [redacted] additional disseminations in oral presentations. The NSA Director briefed the SSCI [redacted] and NSA made a presentation to the FISC [redacted] |  |      |       |       |
|  |  |      |       |       |

~~(TS//SI//NF)~~

(U//FOUO) The S1S Chief or Deputy Chief, two of the approving authorities designated in USSID SP0018, reviews the majority of the requests for disseminating USP information for all NSA authorities, including those unique to BR. Dissemination requests are approved usually the day they are received. Senior Operations Officers (SOO) in the National Security Operations Center (NSOC) are also authorized approvers for disseminating USP information and typically review and approve dissemination requests submitted after hours or in emergency situations.

(U//FOUO) [redacted]

(b)(3)-P.L. 86-36

(U//FOUO) S1S maintains disseminated reports [redacted] signed [redacted] in an access-controlled S1S network folder. Disseminations approved after hours by the SOOs are formally documented, normally the

(b)(1)

(b)(3)-P.L. 86-36

(b)(3)-50 USC 3024(i)

<sup>34</sup> (TS//SI//REL TO USA, FVEY) [redacted]<sup>35</sup> (U//FOUO) [redacted]

TOP SECRET//SI//NOFORN

ST-14-0002

following business day, by SIS. The NSOC Senior Reporting Officer certifies SIS of these disseminations.

(b)(3)-P.L. 86-36

(U//FOUO) Oral briefings that include USP information derived from BR-unique metadata to officials outside NSA occur less frequently. Normally, these briefings are provided by NSA leadership who are approving authorities for disseminating USP information under USSID SP0018. All other BR stakeholders coordinate approvals with one of the approving authorities before presenting information outside NSA. The CT division [redacted] tracks oral briefings only and S1 and S214 track all disseminations of USP information (published and oral), which are included in the 30-day reports filed with the FISC, as the BR Order requires.

- (TS//SI//NF) Dissemination Tracking Requirement The second provision of the BR Order that applies to USP information is the dissemination tracking requirement regarding BR-unique information. NSA tracks and reports to the FISC every instance in which NSA disseminates USP information derived from BR metadata.<sup>36</sup> Approximately every 30 days OOG requests from SIS and S214 the number of disseminated reports containing USP information derived from BR-unique metadata go in input into the 30-day reports filed with the FISC.

[redacted] Although no longer required to track disseminations of foreign person information, S214 continues to track all disseminations of BR-unique information. Disseminations were tracked manually until [redacted] NSA's corporate dissemination tracking tool was implemented [redacted]. Since then, all disseminated reports containing BR-unique information have been tracked in [redacted] completed the upload of [redacted] current and past BR disseminations into [redacted]

(b)(3)-P.L. 86-36

(U//FOUO) Table 18 summarizes the provisions of BR Order 13-158 for sharing and disseminating information derived from BR query results and the controls implemented by NSA to maintain compliance.

<sup>36</sup> (TS//SI//NF) Since 3 September 2009 (BR Order 09-13), NSA has been exempt from reporting in the 30-day reports to the FISC BR disseminations to the executive branch for oversight. On 3 January 2014 (the date the FISC approved BR Order 14-01), this reporting exemption was further extended to include BR disseminations to the legislative branch for oversight.

TOP SECRET//SI//NOFORN

TOP SECRET//SI//NOFORN

ST-14-0002

(U) Table 18. Sharing and Dissemination Provisions and Controls (b)(3)-P.L. 86-36

| Provision   | Control  |
|---|--|
| (U) Results of intelligence analysis queries of the BR metadata may be shared, before minimization, for intelligence analysis purposes among NSA analysts, subject to the requirement that all NSA personnel who receive query results in any form first receive appropriate and adequate training and guidance regarding the procedures and restrictions for handling and disseminating such information.<br><br>(b)(1)<br>(b)(3)-P.L. 86-36 | (U//FOUO) BR stakeholders manually check [redacted] NSA's corporate authorization services tool, to confirm that recipients have [redacted] before sharing BR-unique query results of a USP, in any form.  |
| (U) Before disseminating USP information outside NSA, the NSA Director, the Deputy Director, or one of the officials listed in Section 7.3(c) of USSID SFP0018 must determine that the information identifying the USP is related to CT information and that it is necessary to understand the CT information or assess its importance.   | (U//FOUO) One of the designated approvers (usually the S1S Chief or Deputy Chief) verifies that the CT nexus has been met before disseminating USP information in any form. The approving documentation is independently maintained by S1S for internal recordkeeping and for external review by overseers.  |
| (U) Approximately every thirty days, NSA shall file with the Court a report that among many things includes a statement of the number of instances since the preceding report in which NSA has shared, in any form, results from queries of BR metadata that contain USP information, in any form, with anyone outside NSA.   | (U//FOUO) S1S and S214 independently track the number of disseminations since the preceding report in which NSA has shared, in any form, results from queries of BR metadata that contain USP information, in any form, with anyone outside NSA. ST tracks oral disseminations only. This data collectively is provided to OGC for input into the 300 day reports filed with the FISC. |

**(U) Retention****(U) Provisions of BR Order 13-158**

(U) The BR Order requires that BR metadata be destroyed no later than five years (60 months) after its initial collection.

**(U) NSA's BR age-off process (b)(3)-P.L. 86-36**

(U//SI//NOFORN) To remain compliant with the five year retention requirements NSA completed its first BR age-off [redacted] May 2011.

TOP SECRET//SI//NOFORN

(b)(1)  
(b)(3)-P.L. 86-36

(b)(1)

(b)(3)-P.L. 86-36 (U//~~FOUO~~) Based on guidance from OGC, BR retention compliance is determined using the date when records are received from providers, not the call communication date.

- (U//~~FOUO~~) **Record receipt date** is the date on which providers electronically deliver BR metadata to NSA.
- (U//~~FOUO~~) **Call communication date** is the date on which a telephone call is made from one selection term to another.<sup>38</sup>

**(U) Timing differences with call communication dates and record receipt dates**

(TS//SI//NF)

(b)(1)  
(b)(3)-P.L. 86-36

(b)(3)-18 USC 798

(b)(3)-50 USC 3024(i)

[redacted] Because of these differences, NSA tracks record receipt dates for BR metadata to document compliance with the BR Order. [redacted]

(b)(1)  
(b)(3)-P.L. 86-36  
(b)(3)-50 USC 3024(i)

**(U) Quarantine process**

(TS//SI//NF)

(b)(1)  
(b)(3)-P.L. 86-36  
(b)(3)-18 USC 798  
(b)(3)-50 USC 3024(i)

<sup>37</sup> (U//~~FOUO~~) In September 2013, the DoJ Civil Division directed NSA to preserve all records relating to the collection of BR metadata under the BR FISA program as a result of civil lawsuits against NSA. To comply with the preservation order, NSA did not age-off data with record receipt dates exceeding 60 months in 2014. This data was saved in partitions within NSA system repositories inaccessible to analysts.

<sup>38</sup> (U) Selection terms also refer to identifiers used in dialed number recognition (e.g., telephone numbers).

~~-TOP SECRET//SI//NOFORN~~

ST-14-0002

(U) 2013 age-off

(TS//SI//NF)

(b)(1)  
(b)(3)-P.L. 86-36

## (U//FOUO) Table 19. 2013 BR Age-Off Procedures

(TS//SI//NF)

(b)(1)

(b)(3)-P.L. 86-36

(TS//SI//NF)

## (U) Changes that affected the 2014 age-off

(U//FOUO) In September 2013, DoJ's Civil Division directed NSA not to preserve all records relating to the collection of BR metadata under the BR FISA program as a result of civil lawsuits against NSA. This affected the age-off performed during 2014. BR metadata that would have been aged off to comply with the BR Order was

~~-TOP SECRET//SI//NOFORN~~

~~-TOP SECRET//SI//NOFORN-~~

ST-14-0002

retained to comply with the preservation obligation. This data was saved in partitions within NSA system repositories inaccessible to analysts.

(U//~~FOUO~~) On 12 March 2014, the FISC granted the government's motion for temporary relief from the five year destruction requirement pending resolution of the preservation litigation filed by plaintiffs.<sup>39</sup> As permitted by the BR Order, analysts continue to access for intelligence purposes the [redacted] repository that contains BR metadata received on or after the [redacted] 2010 retention cutoff date using only (I)-P.L. 86-36 RAS approved selection terms.

(TS//SI//NF)

(b)(1)  
(b)(3)-P.L. 86-36  
(b)(3)-50 USC 30224(i))

(b)(1)  
(b)(3)-P.L. 86-36  
(b)(3)-50 USC 30224(i))

39 (TS//SI//NF)

~~-TOP SECRET//SI//NOFORN-~~

TOP SECRET//SI//NOFORN

ST-14-0002

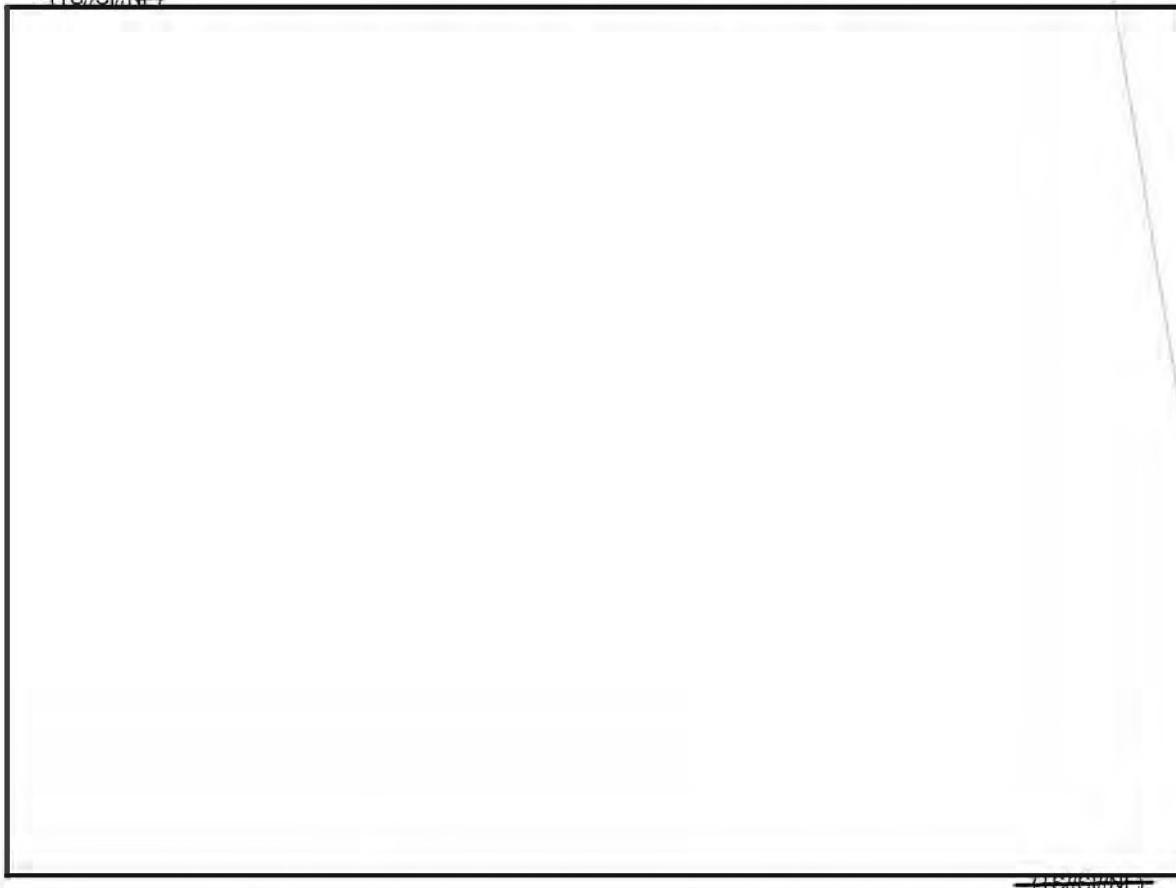
(U//FOUO) Table 20.1

(before and after data comparison)

(b)(1)

(b)(3)-P.L.866386

(TS//SI//NF)



(TS//SI//NF)

(U//FOUO) Table 21 summarizes the provision of BR Order 113-158 for retention and the control implemented by NSA to maintain compliance.

#### (U) Table 21. Retention Provision and Control

(U//FOUO)

| Provision  | Control   |
|--|---|
| BR Metadata must be destroyed no later than five years after its initial collection. | See Table 19 for the procedures performed to age-off BR metadata to comply with the BR Order in 2013. |

(U//FOUO)

#### (U) Oversight

##### (U) Provisions of BR Order 113-158

(U) NSA's OGC and ODOC will ensure that personnel with access to BR metadata receive appropriate and adequate training and guidance regarding the procedures and restrictions for collection, storage, analysis, dissemination, and retention of the BR metadata and the results of queries of the BR metadata. NSA's OGC and ODOC will further ensure that all NSA personnel who receive query results in any form first

TOP SECRET//SI//NOFORN

receive appropriate and adequate training and guidance regarding the procedures and restrictions for handling and disseminating such information. NSA will maintain records of all such training. OGC will provide DDoJ NSD with copies of all formal briefing and/or training materials (including all revisions) used to brief/train NSA personnel concerning this authority.

(U) NSA's ODOC will monitor implementation and use of the software and other controls (including user authentication services) and the logging of auditable information referenced in the previous paragraph.

(U) NSA will ensure that an auditable record is generated whenever BR metadata is accessed for foreign intelligence analysis or accessed using foreign intelligence analysis query tools.

(U) NSA's OGC will consult with DDoJ NSD on all significant opinions that relate to the interpretation, scope, and/or implementation of this authority. When operationally practicable, such consultation will be carried out in advance; otherwise, DDoJ NSD will be notified as soon as practicable.

(U) At least once during the authorization period, NSA's OGC, ODOC, DDoJ NSD, and any other appropriate NSA representatives will meet for the purpose of assessing compliance with the Court's orders. Included in this meeting will be a review of NSA's monitoring and assessment to ensure that only approved metadata is being acquired. The results of this meeting will be reduced to writing and submitted to the Court as part of any application or review or in statu quo authority.

(U) At least once during the authorization period, DDoJ NSD will meet with the NSA's OIG to discuss their oversight responsibilities and assess NSA's compliance with the Court's orders.

(U) At least once during the authorization period, NSA's OGC and DDoJ NSD will review a sample of the justifications for RAS approvals for selection terms used to query the BR metadata.<sup>40</sup>

#### **(U) NSA oversight**

(U//FOUO) In addition to the oversight requirements listed in the BR Order, NSA performs additional oversight, not required in the Order, to ensure compliance. The organizations and the oversight performed are described in the next section.

(U//FOUO) **BR FISA Authority Lead** is the focal point for the BR FISA program within SID, reporting to the CT Associate Deputy Director, who reports to the SID Director. The BR FISA Authority Lead's responsibilities include:

---

<sup>40</sup> (U//FOUO) As of 28 March 2014 (BR Order 14-67), the FISC no longer required OGC and DoJ NSD to conduct periodic reviews of RAS approved selection terms. The government sought this change as a result of the President's directive of 17 January 2014 that NSA submit selection terms to the FISC for RAS approval.

~~-TOP SECRET//SI//NOFORN-~~

ST-14-0002

- (U//~~FOUO~~) Chairing weekly BMD meeting
- (U//~~FOUO~~) Ensuring appropriate program direction and proper program functioning
- (U//~~FOUO~~) Signing NSA's declarations to the FISC during renewal and
- (U//~~FOUO~~) Ensuring that the BR authority is used as described in the BR Order.

(U//~~FOUO~~) Weekly BMD meetings are held to discuss BR FISA program activities to ensure compliance with the BR Order. They include representatives from OGC, ODOC, TV, SW, GTO, DIA, TDC, Counterterrorism Production Center (CTP), IOIG, and other organizations involved in the BR FISA program. Agendas and notes are maintained for each meeting.

(U//~~FOUO~~) **Authorities Integration Group (AIG)** reports directly to the Deputy DIRNSA. The AIG works directly with SIDS and Information Assurance Directorate authority leads, including the BR FISA Authority Lead, and holds weekly meetings with the authority leads and appropriate personnel (e.g. ED, TDC, ODOC, OGC).

(U//~~FOUO~~) The AIG focuses on the activities for each authority, both internal and external, to ensure that they are coordinated and integrated across NSA. The AIG acts as a "forcing function" within NSA by facilitating discussion among the Directorates to promote a better understanding of how decisions affect the various authorities. The AIG provides the Deputy DIRNSA quarterly on each authority.

(U) **ODOC** In 2009, NSA created the position of Director of Compliance to improve the Agency's ability to keep NSA's activities consistent with the laws, policies and procedures designed to protect USP privacy during SIGINT and information assurance missions. ODOC has specific functions with the BR FISA program outlined in the Order. The Assistant Director for Special Compliance Activities is ODOC's representative to the BR FISA program. Some of ODOC's responsibilities include:

- (U) Involvement in all decisions related to the program,
- (U) Participating in weekly BMD meetings,
- (U) Updating BR FISA program training material,
- (U) Participating in quarterly compliance meetings with DDCI, NSDD, and
- (U) Leading the verification of accuracy (VoA) process.

(U//~~FOUO~~) The BR FISA program has been designated as a special compliance activity (SCA) since 2009. This is an NSA mission activity determined to require additional tailored compliance safeguards to ensure the protection of USP privacy. When an activity is identified as an SCA, ODOC becomes active in all aspects of implementing the SCA until it is determined that it is sufficiently underpinned by the Comprehensive Mission Compliance Program and significant risks have been

~~-TOP SECRET//SI//NOFORN-~~

mitigated. The Comprehensive Mission Compliance Program provides a framework and strategy to organize, govern, and resource compliance activities across NSA.

(U//~~FOUO~~) An activity may become an SCA when:

- (U//~~FOUO~~) NSA's external overseers (e.g., DoJ NSD, FISC, Congress) have a heightened sensitivity about an activity or the means by which NSA is executing an activity;
- (U//~~FOUO~~) NSA's legal, policy, compliance, or oversight elements determine that an activity requires attention to understand the application of compliance measures and potential risks; or
- (U//~~FOUO~~) NSA identifies an activity or process that may be out of sync with oversight and compliance regulations and policies, thus making NSA vulnerable to compliance incidents.

(U//~~FOUO~~) Recognizing the critical importance of the completeness and accuracy of documentation filed with external entities, ODOC developed line-by-line accuracy procedures, known as VoA. These procedures provide greater assurance that the representations NSA made to external overseers are accurate and has done a shared understanding among operational, technical, legal, policy, and compliance officials. NSA uses the VoA process during the application process to the Court when requesting renewal of the BR Order.

(U//~~FOUO~~) OGC has specific functions with the BR FISA program outlined in the Order. One requirement is that the OGC consult with DoJ NSD on all significant opinions that relate to the interpretation, scope, or implementation of the authority. The lead OGC BR attorney, assigned from January 2013 to September 2014, stated that OGC consults with DoJ NSD on all significant opinions. OGC saves all correspondence discussing significant legal opinions with DoJ NSD in an access-controlled network folder.

(U//~~FOUO~~) In 2013, NSA OGC met with DoJ NSD at least once during each BR authorization period to review a sample of the justifications for RAS approvals for selection terms issued to query BR metadata. However, as of 28 March 2014 (BR Order 14-67), the FISC no longer required OGC and DoJ NSD to conduct periodic reviews of RAS approved selection terms. The government sought this change as a result of a January 2014 presidential directive enjoining NSA from submitting selection terms to the FISC for RAS approval.

(U//~~FOUO~~) In addition to the OGC's oversight requirements listed in the Order, the OGC defined its BR FISA program responsibilities as:

- (U//~~FOUO~~) Addressing all legal questions from BR FISA program stakeholders;
- (U//~~FOUO~~) Coordinating all interaction with DoJ NSD;

~~TOP SECRET//SI//NOFORN~~

ST-14-00022

- (U//~~FOUO~~) Coordinating the filing of 300 day reports and renewal documents;
  - (U//~~FOUO~~) Leading quarterly compliance reviews with DoJ NSD;
  - (U//~~FOUO~~) Performing First Amendment reviews for USP RAS approval (before 17 January 2014);
  - (U//~~FOUO~~) Coordinating RAS requests and submitting them to DoJ NSD for approval by the FISC (on and after 17 January 2014); and
  - (TS//SI//NF) Approving, with SV, additions of [REDACTED] to the [REDACTED] List.
- (b)(1) ~~~~~ (b)(3)-P.L. 86-36

(U//~~FOUO~~) SV implements the SIGINIT compliance program across NSA, particularly within SID, enabling the SIGINIT mission to operate in compliance with laws, policies, and other guidance. SV provides guidance across the global SIGINIT enterprise, manages compliance incidents, monitors compliance in high-risk areas, resolves problems, and verifies compliance through site visits and audits, and managing the SIGINIT Intelligence Oversight Officer program.

(b)(1) ~~~~~ (b)(3)-P.L. 86-36

(TS//SI//NF) SV performs two main oversight functions for the BR FISA program:

(1) managing access by verifying training requirements semi-weekly for persons who have the [REDACTED] credential and for persons included in the FISABR user group in [REDACTED] and (2) auditing all BR queries performed using query tools by mission and technical personnel to verify compliance with the requirements of the BR Order. SV's process for verifying training and managing access can be found in the Access and Training section.

(b)(3)-P.L. 86-36

(TS//SI//NF) As the BR Order requires, whenever BR metadata is accessed for foreign intelligence analysis or accessed using foreign intelligence analysis query tools, an audit trail record of activity is generated. Although not required by the BR Order, NSA audits all query records. SV verifies that only authorized personnel with the required credentials queried BR metadata, selection terms used to query BR metadata for intelligence analysis were RAS approved at the time of the query, and queries to intelligence analysis maintained within the authorized number of loops from RAS approved seeds as the BR Order requires. For the last two quarters, SV verifies manually that the EAR software system controls are working as intended. SV stated that it has never found an instance of the EAR [REDACTED] allowing an non-compliant query to complete. In 2013, SV audited all [REDACTED] BR query records for that year.

(b)(3)-P.L. 86-36

(U) Additional SV responsibilities include:

(b)(1)

(b)(3)-P.L. 86-36

- (U) Ensuring that SID incident reports are entered timely into NSA's corporate incident reporting database
- (U) Assisting in the development of oversight and compliance courses
- (TS//SI//NF) Providing BR query statistics and [REDACTED] credentialing data for monthly metrics reports provided to SID leadership

~~TOP SECRET//SI//NOFORN~~

TOP SECRET//SI//NOFORN

ST-14-0002

- (U//~~FOUO~~) Maintaining the content and access to the SV BR SharePoint site for storing BR FISA program documentation
- (U//~~FOUO~~) Performing VoAs for statements assigned to SV in the BR Declarations and
- (TS//SI//NF) Approving, with OGC, additions of [REDACTED] (b)(1);  
to the [REDACTED] Approving [REDACTED] List. (b)(1)  
(b)(3) P.L. 86-36

(U//~~FOUO~~) In 2013, SV also assisted DoJ NSD in its periodic review of RAS approved selection terms used for querying BR metadata. SV provided DoJ NSD with RAS justifications and supporting documentation for each review. As previously mentioned in the OGC Oversight section, the periodic reviews of RAS approved selection terms were discontinued pursuant to BR Order 14-67, 28 March 2014.

(U//~~FOUO~~) TV is responsible for identifying, assessing, tracking, and mitigating compliance risks, including USP privacy concerns in NSA Amissions systems across the extended enterprise, including systems that hold BR metadata. TV manages the system compliance certification process, continuous compliance monitoring and technical compliance incident management and conducts training and awareness for technical personnel. TV attends the BMD weekly meetings and performs VoAs for areas assigned to it in the BR Declarations.

(U//~~FOUO~~) OIG conducts audits, special studies, inspections, investigations, and other reviews of programs and operations of NSA and its affiliates. OIG oversight includes:

- b)(3)-P.L. 86-36 [REDACTED]
- (U//~~FOUO~~) Performing audits and special studies of the BR FISA program;
  - (U//~~FOUO~~) Meeting with DoJ NSD at least once during each BR authorization period to discuss oversight responsibilities, NSA's compliance with the BR Order, the status of OIG reviews, and important developments affecting the BR FISA program (notes from these meetings are documented in [REDACTED]);
  - (U//~~FOUO~~) Receiving notification of incident reports for all NSA authorities, including BR FISA, saved in the Agency's corporate incident reporting database;
  - (U//~~FOUO~~) Reviewing Congressional Notifications and notices filed with the FISC of incidents of non-compliance with the BR Order;
  - (U//~~FOUO~~) Preparing Intelligence Oversight Quarterly Reports, in coordination with the DIRNSA and OGC, that summarize compliance incidents for all authorities occurring during quarterly review periods and forwarding the reports to the President's Intelligence Oversight Board through

TOP SECRET//SI//NOFORN

TOP SECRET//SI//NOFORN

ST-14-0002

the Assistant to the Secretary of Defense for Intelligence Oversight (ATSD(IO))<sup>41</sup>;

- (U//FOUO) Performing IO reviews during OIG inspections of joint and field sites;
- (U//FOUO) Attending weekly BMD meetings for situational awareness;
- (U//FOUO) Maintaining the COUCH hotline and responding to complaints of violations of law, rule, or regulation (the OIG also investigates allegations of SIGINT misuse by NSA affiliates operating under the DIRNSA SIGINT authority); and
- (U//FOUO) Reporting immediately to the ATSD(IO) a development or circumstance involving an intelligence activity or intelligence personnel that could impugn the reputation or integrity of the IC or otherwise call into question the propriety of an intelligence activity.

(U//FOUO) The OIG reviews management controls, maintains awareness of compliance incidents, and stays informed of changes affecting NSA authorities, including BR FISA. OIG reviews of the BR FISA program allow it to independently assess compliance with the BBR Order. Since 24 May 2006, that date the original BR Order was signed, the OIG has completed five BR FISA program reviews. Table 22 summarizes OIG reviews of the program.

(U) Table 22. OIG Reviews of the BR FISA program

| Date Issued | OIG Review   | Scope of the Review   |
|-------------|--|---|
| 09/05/06    | Assessment of Management Controls for Implementing the FISC Order: Telephony BR (ST-06-0018) | Reviewed collection, processing, analysis, dissemination, and oversight controls.   |
| 05/12/10    | NSA Controls for FISC BR Orders (ST-10-0004)   | Reviewed querying and dissemination controls; summarized pilot test results for January through March 2010.                     |
| 05/25/11    | Audit of NSA Controls to Comply with the FISC Order Regarding BR (ST-10-0004L)*              | Reviewed querying and dissemination controls; summarized the monthly test results for 2010.                                     |
| 10/20/11    | Audit of NSA Controls to Comply with the FISC Order Regarding BBR Retention (ST-11-0011)     | Verified age-off of BR FISA metadata in 2011 to maintain compliance with the 60 month retention requirement of the BBR Order.   |
| 08/01/12    | NSA Controls to Comply with the FISC Order Regarding BR Collection (ST-12-0008)              | Reviewed collection and sampling controls for ensuring that NSA receives only the BR FISA metadata authorized by the BBR Order. |

\* (U//FOUO) This report summarized monthly test results of the BBR querying and dissemination controls during 2010.

(U//FOUO) et

<sup>41</sup> (U//FOUO) In 2014, the ATSD(IO) was changed to the Office of the Senior DoD Intelligence Oversight Official.

TOP SECRET//SI//NOFORN

## (U) External oversight

(U) DoJ NSD is the liaison between NSA and the FISC for the BR FISA program. DoJ NSD oversight includes the following:

- (U) Coordinating 90-day renewal applications
- (U//FOUO) Providing guidance to NSA OGC on all significant legal opinions relating to the interpretation, scope, and implementation of the BR authority
- (U//FOUO) Reviewing NSA briefings and training transcripts to ensure that they accurately describe the requirements of the BR Order before NSA incorporates material into its training program (e.g., OVSCI205, OVSCI206)
- (U//FOUO) Meeting with NSA's OIG at least once during each BR authorization period to discuss oversight responsibilities and NSA compliance with the BR Order. Proposed initiatives and other important developments affecting the BR FISA program are discussed with the OIG
- (U) Meeting with NSA's OGC, ODOC, and other NSA stakeholders at least once during BR authorization periods to assess compliance. DoJ NSD meets with OGC, ODOC, and the BR FISA Authority Lead to review the Quarterly Compliance Report that summarizes the results of weekly tests NSA performed to ensure that NSA is receiving only authorized data. DoJ NSD submits summaries of these meetings in writing to the FISC as part of applications to renew the authority.

-(TS//SI//NF) In 2013, DoJ NSD met with NSA OGC and SV at least once each BR authorization period to review a sample of the justifications for RAS approvals for selection terms used to query BR metadata. For RAS selection terms approved in 2013, DoJ NSD sampled 100 percent of the USP RAS selection terms and 20 percent of the foreign RAS selection terms. As mentioned in the OGC Oversight section, DoJ NSD and OGC's periodic reviews of RASS selection terms were discontinued pursuant to BR Order 14-67, dated 28 March 2014. NSA now submits selection terms to the FISC for RAS approval to comply with the President's January 2014 directive. Table 23 summarizes DoJ NSD sampling of RASS selection terms approved in 2013.

(U//FOUO) Table 23. DoJ NSD Sample of RAS Selection Terms

Approved in 2013

(b)(1)

(b)(3)-P.L. 86-36

\* (U//FOUO) Estimate calculated using DoJ NSD sampling methodology (sample 20 percent of foreign selection terms for review).

† (U//FOUO) Data includes RAS selection terms that may have been approved more than once in 2013.

20%\*\*\*

(TS//SI//NF)

TOP SECRET//SI//NOFORN

ST-14-0002

(U//FOUO) ODNI representatives attend DoJ NSD meetings with NSA's OGC, ODOC, and the BR FISA Authority Lead to review the Quarterly Compliance Report. Although ODNI does not have a formal role described in the BR Order, it participates in its general role as an overseer of IC activities.

~~(C//REL TO USA, FVEY)~~ FISC is the approving authority for all renewals, amendments, reinstatements of the BR authority, and, starting in February 2014, RAS for selection terms NSA submitted. If the FISC approves the BR Primary Orders that authorize NSA to acquire bulk BR FISA metadata and the BR Secondary Orders that compel providers to provide daily bulk BR FISA metadata to NSA for the duration of the Order. The FISC performs oversight by receiving filings of Rule 13(a) Notices, Correction of Material Facts, and Rule 3(h)(b) Notices; Disclosure of Non-Compliance, by DoJ NSD on behalf of NSA. The FISC also reviews the 30-day renewal applications and 30-day reports that NSA files. The 30-day reports document NSA application of the RAS standard (which applies after March 2014); NSA's implementation and operation of the automated query process (which applies after March 2014—NSA never implemented this process and withdrew its request to do so); NSA's description of significant changes in the way in which the BR metadata is received from providers and significant changes to the controls NSA has in place to receive, store, process, and disseminate BR metadata and the number of instances since the preceding report that NSA disseminated, in any form, USP information outside NSA. The 30-day reports also include NSA's attestation that the CT nexus was completed and disseminations were approved by a designating approving authority before disseminating USP information derived from BR-unique metadata.

(U) Table 24 summarizes the provisions of BR Order 13-158 for oversight and the controls implemented by NSA to maintain compliance.

(U) Table 24. Oversight Provisions and Controls

(U//FOUO)

| Provision   | Control   |
|---|---|
| NSA's OGC and ODOC will ensure that personnel with query access to BR metadata receive appropriate and adequate training and guidance regarding the procedures and restrictions for collection, storage, analysis, dissemination, and retention of the BR metadata and the results of queries of the BR metadata. |   |
| NSA's OGC and ODOC will ensure that all NSA personnel who receive query results in any form first receive appropriate and adequate training and guidance regarding the procedures and restrictions for the handling and dissemination of such information.  | See Table 14—Access and Training Provisions and Controls. |
| NSA will maintain records of all such training.   |   |
| OGC will provide DoJ NSD copies of all formal briefing and training materials (including all revisions) used to train NSA personnel concerning the authority.   |   |

TOP SECRET//SI//NOFORN

|  |   |
|--|---|
| NSA's ODOC will monitor implementation and use of software and other controls (including user authentication services) and the logging of auditible information referenced above.  | SV performs 100 percent audits of queries performed using query tools by mission and technical personnel to verify that only authorized personnel who have the required credentials queried BR metadata, selection terms used to query BR metadata for intelligence analysis purposes were RAS approved at the time of the query, and queries for intelligence analysis purposes remained within the number of authorized hops from RAS approved seeds. |
| NSA's OGC will consult with DoJ NSD on all significant opinions that relate to the interpretation, scope, and/or implementation of this authority.   | NSA OGC confirmed that NSA has always consulted with and received advance approval from DoJ NSD and the FISC before implementing significant changes to the BR FISA program. NSA OGC saves all correspondence with DoJ NSD in an access-controlled network folder.  |
| At least once during the authorization period, NSA's OGC, ODOC, DoJ NSD, and any other appropriate NSA representatives will meet to assess compliance with the Court's orders. Included in this meeting will be a review of NSA's monitoring and assessment to ensure that only approved metadata is acquired. The results of this meeting will be reflected in the RAS application submitted to the Court as part of any application to renew or reinstate the authority. | DoJ NSD meets with OGC, ODOC, and the BR Lead to review the Quarterly Compliance Report, which summarizes the results of weekly tests performed by NSA to ensure that it is receiving only the BR metadata authorized by the Order. DoJ NSD submits summaries of these meetings in writing to the FISC as part of the applications to renew the authority.<br><br>(b)(3)-P.L. 86-36   |
| At least once during the authorization period, DoJ NSD will meet with the NSA's OIG to discuss their respective oversight responsibilities and assess NSA's compliance with the Court's orders.  | NSA OIG meets with DoJ NSD at least once during BR authorization periods to discuss oversight responsibilities and NSA's compliance with the requirements of the Order. Notes from these meetings are documented in [redacted]  |
| At least once during the authorization period, NSA's OGC and DoJ NSD will review a sample of the justifications for RAS approvals for selection terms used to query the BR metadata.   | In 2013, NSA OGC and SV met with DoJ NSD at least once during BR authorization periods and review a sample of the justifications for RAS approvals for selection terms used to query the BR metadata.*  |

\* As of 28 March 2014 (BR Order 14-67), the FISC no longer required OGC and DoJ NSD to conduct periodic reviews of RAS approved selection terms. The government sought this change as a result of the President's January 2014 directive under which NSA began submitting selection terms to the FISC for RAS approval.

(U//FOUO)

### (U) BR FISA Program Incidents of Non-Compliance

(U//FOUO) FISC Rules of Procedure require that NSA "provide corrections of material facts" and "disclosures of non-compliance" with FISC Orders. NSA also must determine whether Congressional notifications are required. Our review focused on the process for identifying and reporting incidents of non-compliance, the incidents reported in 2013 to the Court and other external observers and the controls NSA has instituted to mitigate recurrence of compliance incidents.

~~TOP SECRET//SI//NOFORN~~

ST-14-0002

**(U) FISC Rules of Procedure**

(U) The FISC Rules of Procedure, 11 November 2000, adopted pursuant to 50 U.S.C. § 1803(g), govern FISC proceedings. Rule 13, *Correction of Misstatement or Omission; Disclosure of Non-Compliance*, is the procedure that NSA follows when notifying the Court, through DoJ NSD, of BR FISA misstatements and compliance incidents.

**(U) Rule 13(a) Correction of Material Facts** If the government discovers that a submission to the Court contained a misstatement or omission of material fact, the government must immediately, in writing, inform the Judge to whom the submission was made off:

- (1) (U) the misstatement or omission;
- (2) (U) necessary corrections;
- (3) (U) the facts and circumstances relevant to the misstatement or omission;
- (4) (U) modifications the government has made or proposes to make in how it will implement any authority or approval granted by the Court; and
- (5) (U) how the government proposes to dispose of or treat information obtained as a result of the misstatement or omission.

**(U) Rule 13(b) Disclosure of Non-Compliance** If the government discovers that any authority or approval granted by the Court has been implemented in a manner that did not comply with the Court's authorization or approval with a justifiable delay, the government must immediately, in writing, inform the Judge to whom the submission was made off:

- (1) (U) the non-compliance;
- (2) (U) the facts and circumstances relevant to the non-compliance;
- (3) (U) modifications the government has made or proposes to make in how it will implement any authority or approval granted by the Court; and
- (4) (U) how the government proposes to dispose of or treat information obtained as a result of the non-compliance.

**(U) Identifying and Reporting Incidents of Non-Compliance****(U) Identifying incidents of non-compliance**

(U//FOUO) NSA typically discovers incidents of non-compliance with the BR Order during its operation of the BR FISA program. Because of the program's sensitivity, suspected anomalies are reported out of an abundance of caution. Training, a pillar of the compliance framework, provides heightened sense of awareness for personnel to identify potential violations of the BR Order. A second pillar, monitoring and assessment, includes manual and technical controls to detect abnormalities. A weekly BMD meeting, attended by BR FISA program stakeholders, provides a forum for addressing potential problems.

(U//FOUO) When a possible incident is discovered, it is communicated to the BR FISA Authority Lead OGC, ODOC, SV, and, if appropriate, TV and S2. BR FISA program stakeholders meet to discuss the facts and determine, with OGC's concurrence, whether a potential violation of the Order has occurred. If OGC believes an incident has or may have occurred, even if all the facts have not been

~~TOP SECRET//SI//NOFORN~~

gathered, preliminary notification to DoJ NSD is made shortly after notice to the DIRNSA, other NSA leadership, BR FISA program stakeholders, and OIG. Upon receiving initial notification from OGC, DoJ NSD starts drafting a preliminary notification to the Court.

(U//FOUO) Once the facts have been gathered and OOGC has made an initial determination that a violation of the BIR Order has occurred, OOGC finalizes a notification of non-compliance and forwards it to DoJ NSD, which makes the final determination as to whether there has been an incident of non-compliance that must be reported to the FISC. If DoJ NSD determines that an incident has occurred, it prepares a draft notification to the Court, coordinates the notification with NSA, finalizes the draft, and files the notification with the Court.

(U//FOUO) DoJ NSD often files a preliminary notification with the Court and, if needed, will follow up later with additional notifications. In some cases, the preliminary notification of an incident serves as the final notice. More than one notice to the Court to address an incident is typically required when at the time of the preliminary notification:

- (U//FOUO) NSA does not have all the facts the Court needs to fully understand or address the incident or
- (U//FOUO) Remedial follow-on action may be needed.

(U//FOUO) For the four incidents of non-compliance first reported to the Court in 2013, two required additional information; therefore, final notices were filed separately. One of the incidents included a notice of material misstatement because NSA had previously filed a declaration to the Court that contained inaccurate information.

#### **(U) Congressional notifications**

(U//FOUO) In addition to the requirement to notify the FISC, DIRNSA has a statutory obligation to keep the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence fully and currently informed of all significant intelligence activities.<sup>42</sup> NSA nevertheless doubts about notification in favor of notification. In addition to notifying Congress and the Director of National Intelligence (DNI), DIRNSA must notify the Undersecretary of Defense for Intelligence (USD(I)) and other USD(I) staff, as USD(I) guidance directs. For all BIR FISA incidents of non-compliance reported by Congressional notifications to the intelligence committees, NSA also notifies the Senate and House Committees on the Judiciary.

(U//FOUO) NSA's Legislative Affairs Office (LAO) manages NSA's liaison with the Congress and DNI, DoD, the IIC, and other U.S. government departments and agencies regarding matters of concern to the Congress. LAO is NSA's focal point for

---

<sup>42</sup> (U) See 50 U.S.C. §3091, as implemented by Intelligence Community Directive 12, *Congressional Notification*, 16 November 2011.

~~-TOP SECRET//SI//NOFORN~~

ST-14-0002

Congressional inquiries, correspondence, questions from the media, and RFRF incidents directed to NSA.

(U//FOUO) NSA Policy 1-333, *Relations with the Congress*, 22 July 2005, provides guidelines for identifying matters that OGC and AOG must consider reporting to the Congressional intelligence committees under 50 U.S.C. §§3091 and 3092. The guidelines do not constitute a comprehensive list of what must be reported. Compliance incidents are assessed under a general guidance to consider for reporting matters that the intelligence committees have expressed a continuing interest in or which otherwise qualify as significant intelligence activities or failures.

(U//FOUO) NSA works to keep Congressional intelligence committees fully and currently informed about the Agency's activities, one of which is required under the guidelines outlined in NSA/CSS Policy 1-33.

(U//FOUO) OGC's analysis of the incidents of non-compliance that occurred in the BR FISA program in 2013 resulted in three of the four incidents reported as Congressional notifications.

#### **(U) 2013 Bidirectional Non-Compliance**

(U//FOUO) In 2013, NSA reported four incidents of non-compliance to the Court. The following are NSA's reports of the incidents and the actions NSA took to mitigate recurrence.

~~(TS//SI//NF)~~ Notice of Compliance Incident [REDACTED] (b)(3) P.L. 86-36  
 [REDACTED]

~~(TS//SI//NF)~~ [REDACTED] An NSA analyst conducted a query of the BR metadata with a RAS approved U.S. person selection term (the U.S. person is currently subject to Court-authorized electronic surveillance). [REDACTED]  
 [REDACTED] The query yielded [REDACTED] new identifiers believed to be used by the same U.S. person as the selection term. The analyst then sent those [REDACTED] U.S. person identifiers, for further tasking, to an e-mail alias that timetabled NSA personnel who had not completed the required BR metadata training to receive query results containing U.S. person identifiers. The analyst also entered the [REDACTED] identifiers into certain analytic and tasking tools to which NSA personnel without the required BR metadata training have access.

~~(TS//SI//NF)~~ The same day, the analyst's NSA supervisor realized that the [REDACTED] U.S. person identifiers had been shared, within NSA, with analysts who had not received the training required to receive them. The supervisor took steps to immediately de-task the identifiers, delete them from the analytic tools, and recall the e-mail message, processes which had been successfully accomplished on about March 22, 2013. The analytic and tasking tools had retained data collection artifacts, and a follow-up e-mail was sent to all addresses on the e-mail alias instructing that anyone without the required training should destroy all copies of the original e-mail sent to the alias.

[REDACTED] notification was required for this

~~-TOP SECRET//SI//NOFORN~~

~~(TS//SI//NF)~~ Controls put in place to mitigate recurrence The BR Order requires that results of queries of BR metadata may be shared among NSSA analysts for intelligence analysis before minimization, subject to the requirement that all NSSA personnel who receive query results in any form first receive appropriate and adequate training and guidance regarding the procedures and restrictions of handling and disseminating such information. Analysts who run queries and obtain results on BR metadata receive annual OWSCLI205 training regarding the rules and restrictions on sharing BR metadata query results. Before analysts share BR-derived query results containing USPI information, they must confirm that the recipient has the [redacted] credential to receive BR metadata information. Analysts are reminded to verify recipient's credentials [redacted]. To help mitigate recurrence, the analyst's supervisor reiterated to the analyst the requirements for sharing BR metadata query results and the portions of the OWSCLI205 training related to sharing.

(b)(1)  
(b)(3)-P.L. 86-36

~~(TS//SI//NF)~~ Notice of Compliance Incident [redacted]  
(b)(3)-P.L. 86-36 [redacted]

(b)(1)  
(b)(3)-P.L. 86-36

~~(TS//SI//NP)~~ [redacted] NSA technical personnel discovered that NSA had inadvertently retained files containing call detail records that were more than five years old. Specifically, these call detail records, which had been produced pursuant to the Court's Primary Orders, [redacted]. These call detail records were among those used in connection with migration of call detail records to a new system [redacted]. See Declaration, Docket Number BBR-JL-557 at 13 n.8 (describing migration of records to a replacement system). The call detail records could be accessed or used by only technical personnel who had received appropriate and adequate training to access call detail records..

~~(TOP SECRET//SI//NF)~~ [redacted] NSA technical personnel destroyed the call detail records used in the migration of records that had been inadvertently retained past the retention limit of five years. As a result of the destruction, NSA is unable to provide an estimate regarding the volume of data destroyed. For recovery back-up purposes, NSA has retained those call detail records used in the migration of records that did not exceed the retention limit, and will use those records in accordance with the requirements of the Court's Primary Orders.

~~(TS//SI//NF)~~ On 7 May 2013, NSA submitted a Congressional notification of the compliance incident to the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence and the House and Senate Committees on the Judiciary. Copies were also provided to Congressional affairs offices at the ODNI, USD(I), and DOL. On 7 May 2013, the NSSA OIG notified the ASD(DOIO) of the incident and Congressional notification.

(b)(3)-P.L. 86-36

~~(TS//SI//NF)~~ Controls put in place to mitigate recurrence In response to this incident, technical personnel developed a script that searches for ingest and backup files in [redacted] servers containing BR metadata older than four years, 11 months. Before the preservation order, if such files were identified, the script would send automated reminders weekly for three weeks and then daily until the file date been

~~TOP SECRET//SI//NOFORN~~

ST-14-0002

(b)(3)-P.L. 86-36 manually deleted.<sup>43</sup> No files matching the criteria have been identified since the script was developed. Before the preservation order, the [REDACTED] database, which ingests files from the [REDACTED] servers, automatically deleted files before they reached the five-year mark. NSA maintains location restrictions for matching search and directories that hold BR metadata files.

~~(TS//SI//NF)~~ Notice of Compliance Incidents [REDACTED]

(b)(1) (b)(3)-P.L. 86-36 ~~(TS//SI//NF)~~ Preliminary [REDACTED] NSA informed the NSD's Office of Intelligence (OI) that, in the course of reviewing its formal reporting to the IFSC, it had identified BR metadata products containing U.S. person information that it had not reported in thirty-day reports to the Court. These disseminations [REDACTED]

[REDACTED] For each BR metadata product, an authorized official made the required CT determination prior to dissemination. NSA and OI continue to investigate the facts and circumstances concerning this matter and the DoJ will provide a thorough explanation of this matter to the Court.

(b)(3)-P.L. 86-36

~~(TS//SI//NF)~~ Final [REDACTED] final notice of Compliance Incidents, [REDACTED] was filed with the Court. The notice indicated that the disseminations [REDACTED] in total — were not included in the thirty-day reports because at the time the incidents occurred [REDACTED] NSA relied on a single individual to keep reports of disseminations that occurred during each reporting period and IQ provided information about those disseminations for inclusion in the thirty-day reports. Incidentally, the disseminations described above were not recorded and, as result, information about them was not included in the thirty-day reports. Currently, as discussed in a notice in this matter filed with the Court [REDACTED] NSA's Information Sharing Services (ISS) office maintains records of the CT determinations for each disseminated BR metadata product containing U.S. person information. NSA's ISS now also verifies the accuracy of statements regarding disseminations that are included in each thirty day report by confirming that its records reflect the number of disseminations described in each report.

~~(TS//SI//NF)~~ Along with the final notice, as supplemental report to the Court provided additional details and NSA's attestation that, based on dissemination of the USP information was determined to be related to CT information and necessary to understand the CT information or to assess its importance.

~~(TS//SI//NF)~~ On 20 September 2013, NSA submitted a Congressional notification of the compliance incident to the House Permanent Select Committee on Intelligence, the Senate Select Committee on Intelligence, and the House and Senate Committees on the Judiciary. Copies were also provided to the Congressional Affairs offices at ODNI, USDI(I), and DoJ. On 12 September 2013, the NSA OIG notified the ATSD(IQ) about the incident and providing Congress a final notification.

<sup>43</sup> (U//FOUO) On 21 March 2014, the U.S. District Court for the Northern District of California issued a preservation order against the destruction of BR metadata.

~~TOP SECRET//SI//NOFORN~~

TOP SECRET//SI//NOFORN

ST-14-0002

(b)(3)-P.L. 86-36

(TS//SI//NF) Controls put in place to mitigate recurrence. In response to this incident, [REDACTED] NSA issued the "BR FISA Reporting Process SOP" that documents external reporting requirements and organizational responsibilities and defines a standardized, repeatable process of collection coordination and release of mandatory FISC reports for the BR FISA program. The SOP states that as part of incident remediation, the BR program committed to refine the manual report process and create a software tool, [REDACTED] to help automate accounting of BR EISA disseminations.

(U//FOUO) [REDACTED] NSA's corporate dissemination tracking tool was implemented in December 2013. Before this, disseminations were tracked manually. Since then, all disseminated reports derived from BR metadata have been tracked in [REDACTED]

(b)(1)  
(b)(3)-P.L. 86-36

(TS//SI//NF) Preliminary [REDACTED] NSA notified the NSD's OI that [REDACTED] [REDACTED] ~1 [REDACTED] NSA received [REDACTED] [REDACTED] a sample? [REDACTED]  
call detail records for testing purposes.

(b)(1)  
(b)(3)-P.L. 86-36  
(b)(3)-50 USC 3024(i)

(TS//SI//NF) NSA deleted all [REDACTED] call detail records [REDACTED] Prior to its destruction, the [REDACTED] was stored at all times on servers accessible only to technical personnel and was not available for intelligence analysis. NSA and OI continue to investigate the facts and circumstances concerning this matter and the DoJ will provide a thorough explanation of the matter to the Court upon completion of the investigation.

(b)(1)  
(b)(3)-P.L. 86-36

(TS//SI//NF) Final [REDACTED] [REDACTED] (Complaint & OI) (Complaint & OI) [REDACTED] [REDACTED] was filed with the Court. NSA identified [REDACTED] in the sample [REDACTED] call detail records [REDACTED] L... L..., [REDACTED]

(b)(3)-P.L. 86

(TS//SI//NF) On 17 December 2013, NSA submitted a Congressional notification of the compliance incident to the House Permanent Select Committee on Intelligence, Senate Select Committee on Intelligence, and the House and Senate Committees on the Judiciary. Copies were also provided to the Congressional affairs offices at the ODNI and USSDI. On 2 December 2013, the NSA OIG notified the ATSSD(OI) of the incident and pending Congressional notification.

TOP SECRET//SI//NOFORN

~~TOP SECRET//SI//NOFORN~~

ST-14-0002

(TS//SI//NF) Controls put in place to mitigate recurrence NSA filed a "Notice of Material Misstatement" because in a previous declaration to the Court, NSA stated that it had expected to receive sample [redacted] records [redacted]

(b)(1) (b)(3)-P.L. 86-36 (b)(3)-50 USC 3024(i)

[redacted] for testing and that NSA had notified the providers that it did not want CSLI information. NSA was not able to verify [redacted]. As an implementing control, NSA modified the way it performs the VoA on the declaration to the Court so that all organizations associated with the BR FISA program participate in the VoA process and review the entire document. The BR FISA Authority had initiated quarterly meetings with stakeholders to compare the previous final BR Order with the new declaration to identify changes and ensure that the new declaration is reviewed for accuracy. Since the incident, NSA has not received sample [redacted] records [redacted]

(TS//SI//NF) As discussed in the Sampling section, PIAs test the [redacted] feed daily and weekly to verify that it does not contain CSLI data. The PIA [redacted] identified no CSLI data since the [redacted] feed became operational [redacted]

(U//FOUO) The four incidents of non-compliance were included in NSA's first, third, and fourth quarters 2013, *Report to the Intelligence Oversight Board on NSA Activities*.

(U//FOUO) For a list of the incidents of non-compliance from 2010 through 2012, see Appendix B.

## **(U) NSA Use of the BR FISA Authority**

---

(U//FOUO) Although no formal process has been implemented to assess the effectiveness of the BR FISA authority, NSA asserts that the authority has made valuable contributions to the CT intelligence mission and that it plays an important role for NSA intelligence analysts tasked with identifying potential terrorist threats to the U.S. homeland and U.S. interests abroad.

### **(U) Methods Used to Assess Effectiveness**

(U) NSA's BR FISA program was developed to assist the U.S. government in detecting communications between known or suspected terrorists operating outside the United States and others inside the United States, as well as communications among operatives within the United States. The 9/11 Commission identified that detecting and linking such communications as a critical intelligence gap in the aftermath of the attacks on 11 September 2001.

(TS//SI//NF) Based on requests from the Senate Select Committee on Intelligence to determine the "value of the program," NSA and FBI personnel developed in February 2014 the "BR FISA Bulk Metadata NSA/FBI Process for FBI Feedback" plan that describes NSA's responsibility to deliver to the FBI spreadsheets with BR information and the FBI's responsibility to summarize use for NSA. The plan called for FBI's [redacted] to categorize selection terms in the BR FISA report as follows:

(b)(1)  
(b)(3)-P.L. 86-36

~~TOP SECRET//SI//NOFORN~~

- (U//~~FOUO~~) Not of interest as the selection term is technically flawed or the characteristics make it worthless for research.
- (U//~~FOUO~~) Known to the FBI-FBII is aware of the selection term independently.
- (U//~~FOUO~~) Known to the FBI with additional information -FBII is aware of the selection term and potentially, but NSA is preparing to provide amplifying information to aid FBI investigations.
- (U//~~FOUO~~) Unknown to the FBI-the FBI was not aware of the selection term.

(TS//SI//NF) Under the plan, [redacted] would send BR-unique leads to FBI field offices. [redacted]

(b)(1)  
(b)(3)-P.L. 86-36

(U//~~FOUO~~) [redacted]

(b)(3)-P.L. 86-36

(U//~~FOUO~~) BR FISA program leadership recognizes that there is no process to track program effectiveness. They agreed on the need to track effectiveness but were unable to determine how to do so. Feedback is difficult to obtain. One former BR FISA program leader asked, "How do you assess the effectiveness of an authority when we don't get feedback from the customer?"

(TS//SI//NF) Another limitation on NSA's ability to determine the effectiveness of the BR FISA program [redacted]

(b)(1)  
(b)(3)-P.L. 86-36

TOP SECRET//SI//NOFORN

ST-14-0002

(U) Table 25. Selection Terms in Approved Status as of 31 December 2013  
by Target Office of Primary Interest(b)(1)  
(b)(3)-P.L. 86-36

(TS//SI//NOFORN)

(6435B) (b)(3)-P.L. 86-36

(U//FOUO)

(b)(3)-P.L. 86-36 NSA implemented the "BR FISA Bulk Metadata Monthly Internal Report for SID." The report includes:

- [REDACTED]
- [REDACTED]
- (U//FOUO) Number of approved RAS selection terms,
- (U//FOUO) Number of queries,
- (U//FOUO) BMD volume, and
- (U//FOUO) Number of personnel by organization and work role with program access, approved to disseminate USSP information, and approved as HMCs.

**(U) Contributions from FISA Authority to Support Intelligence Mission****(U) 2013 highlights**

(TS//SI//NOFORN) NSA does not assert that information from the BR FISA program does, by itself, identify or thwart threats. Instead, information obtained through the program plays a complementary role within a large body of intelligence and CT investigations. It is important to note that BR metadata may sometimes be the single source of intelligence. However, typically, acquisition and analysis of BR metadata are designed to fill gaps in information gathered under other collection authorities. By helping close those gaps, NSA personnel report that BR data contributes to comprehensive efforts to identify and address threats to the homeland. The following are highlights from the BRFISA program in 2013.

- (TS//SI//NOFORN) [REDACTED]

(b)(1)  
(b)(3)-P.L. 86-36  
(b)(3)-18 USC 798  
(b)(3)-50 USC 3024(i)

TOP SECRET//SI//NOFORN

- (TS//SI//NOFORN)

(b)(1)  
(b)(3)-P.L. 86-36  
(b)(3)-18 USC 798  
(b)(3)-50 USC 3024(i)

(U) On 21 June 2013, in response to a request from the House Permanent Select Committee on Intelligence after unauthorized public disclosure series, NSA provided to that committee and the Senate Select Committee on Intelligence, the House and Senate Committees on the Judiciary, and the Defense subcommittees of the House and Senate Appropriations Committees a list of 54 events in which the BR FISA or FAA §702 authorities or both contributed to the production of SIGINT and to the IC's understanding of terrorism activities.

#### **(U) Analysis of the Authority**

(U//~~FOUO~~) NSA senior management believe that the BR FISA program is important to intelligence analysts tasked with identifying potential terrorist threats to the U.S. homeland, primarily in support of the FBI, by enhancing their ability to detect, prioritize, and track terrorist operatives and their support networks in the United States and abroad. By querying BR metadata, intelligence analysts are able to:

- (U//~~FOUO~~) Detect domestic and foreign selection terms in contact with domestic and foreign selection terms associated with foreign terrorist organizations,

(b)(3)-P.L. 86-36

~~TOP SECRET//SI//NOFORN~~

ST-14-0002

- (U//~~FOUO~~) Discover selection terms with which the foreign and domestic selection terms associated with foreign terrorist organizations are in contact, and
- (U//~~FOUO~~) Detect possible terrorist related communications between communicants inside the United States.

**(U) Identifying threats**

(U//~~FOUO~~) NSA has many sources of information that provide indications of potential terrorist activity against the United States and its interests abroad. The best analysis typically occurs when analysts evaluate information obtained from all those sources to disseminate to the FBI and the IC as complete a picture as possible of potential terrorist threats. Although BR metadata is not the sole source of information available to NSA CT personnel, it is a component of the information that analysts rely on to execute threat identification and characterization. BR metadata can add to the IC's and law enforcement community's understanding and evaluation of threat information and the need to take investigative action.

**(U) Agility**

(U) BMD, NSA personnel assert, enables the Agency to quickly analyze communications and contact chains. Unless the data is aggregated, it may not be feasible to detect communication chains that cross communication networks and authorities. The ability to query accumulated metadata from multiple authorities significantly increases NSA's ability to rapidly detect persons who are affiliated with foreign terrorist organizations and might otherwise go undetected.

**(U) Hops**

(U//~~FOUO~~) When NSA performs a contact chaining query on a terrorist associated selection term, analysts are able to detect not only the direct contacts made by that first tier of contacts but also the additional tiers of contacts, out to the maximum number of permitted hops from the seed selection term. [REDACTED]

(b)(3)-P.L. 86-36

[REDACTED]  
provides a more complete picture of those who associate with terrorists or are engaged in terrorist activities. The ability to look at a network beyond the first hop enables analysts to potentially identify the core of a network, focusing and prioritizing resources effectively against threats.

**(U) Historical data**

~~(TS//SI//NF)~~ And the advantage that SID leadership ascribes to the BR FISA program is that the BR metadata is historical. [REDACTED]

[REDACTED] historical connections are critical to understanding newly identified targets, and metadata may contain links that are unique, pointing to potential targets of interest that may otherwise be missed.

(b)(1)  
(b)(3)-P.L. 86-36~~TOP SECRET//SI//NOFORN~~

(U) **Tradecraft**

(U//~~FOUO~~) Analysts report that BR metadata analysis facilitates the understanding of the communications tradecraft of terrorist operatives who may be [REDACTED] conduct attacks against the United States. [REDACTED]

[REDACTED]

(b)(3)-P.L. 866366

(U) **Complementary**

(U//~~FOUO~~) The BR FISA program, SID leadership asserts, complements information that NSA collects by other means, increasing the value to the Agency and linking possible terrorist-related telephone communications between communicants based solely inside the United States. As a complementary tool to other intelligence authorities, the NSA's access to BR metadata increases the likelihood of detecting terrorist cell contacts within the United States. The BR FISA program provides NSA the information necessary to perform call chaining that can enable analysts to obtain a much broader understanding of the target and, as a result, allow NSA to provide to the FBI and the IC a more complete picture of possible terrorist-related activity inside the United States.

(b)(3)-P.L. 866366

(U) **Prioritizing**

(U//~~FOUO~~) The BR FISA program assists with applying limited analytic and linguistic resources available to the CT mission [REDACTED] have the highest probability of connection to terrorist targets. Analysis of BR metadata can help analysts prioritize communications of non-USPs that it acquires under other authorities because such persons are of heightened interest if they are in a communication network with persons in the United States.

(b)(3)-P.L. 86-36

(U//~~FOUO~~) SID leadership asserts that, without the ability to obtain and analyze BR metadata, NSA would lose a tool for detecting communication chains that link to selection terms associated with known and suspected terrorist operatives, which can lead to the identification of previously unknown persons of interest. The BR FISA program allows efficient [REDACTED]

[REDACTED] potential terrorist activities. Any other means that might be used to conduct similar analyses would require multiple, time-consuming steps that would frustrate rapid analysis in challenging situations and could fail to capture some information available through BR metadata. If BR metadata is not aggregated and retained for a time, NSA could not detect [REDACTED]

[REDACTED]

(U) Former DIRNSA General Alexander testified to the Senate Committee on the Judiciary in December 2013:

(U) Measuring the value of the BR FISA authority by the number of plots exposed to date misses the point and presents us with a false choice. The BR FISA authority is similar to an insurance policy, designed to make sure that the gap proposed after 9/11 doesn't happen again, with perhaps even more catastrophic consequences. As with an insurance

**ST-14-0002**

[REDACTED]

policy on your house, you don't determine its value by asking down many times you've collected on the policy to date - you want to have it for the possible fire, or flood, or theft in the future. Combined with the limitations on the program, the potential benefit in allowing us to uncover the hidden terrorist in the U.S. still provides a unique value consistent with the protection of privacy rights.

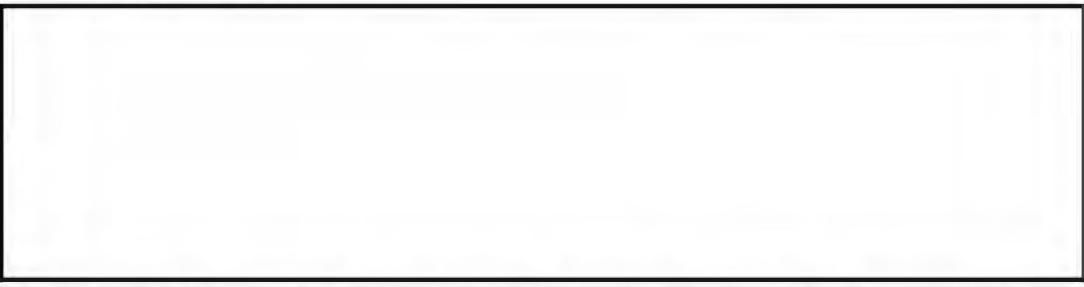
## III. (U) FAA §702

## (U) Background

## (U) The FAA §702 certifications

~~(S//NF)~~ Section 702 of ~~FAA~~, *Procedures for Targeting Certain Persons Outside the United States other than United States Persons*, states that the Attorney General and the DNI may jointly authorize, for the period of up to one year, the targeting of persons who are not USPs and who are reasonably believed to be located outside the United States to acquire foreign intelligence information. This authority is granted on the basis of annual certification made by the Attorney General and the DNI to the NSC. [redacted] certifications identify categories of foreign intelligence information sought through this acquisition:

(b)(1)  
 (b)(3)-P.L. 86-36  
 (b)(3)-50 USC 3024(i)



~~(S//NF)~~ The NSA targeting and minimization procedures establish the processes that the Agency must follow and the requirements that it must satisfy to comply with the limits the statute and the Constitution impose on the use of this surveillance. The targeting procedure must be "reasonably designed" to limit acquisition under the [redacted] FAA §702 certifications to non-USPs reasonably believed to be located outside the United States to acquire foreign intelligence information and to prevent intentional acquisition of communications in which the sender and all intended recipients are known at the time of acquisition to be in the United States.<sup>45</sup> The purpose of the minimization procedures is to establish controls over the acquisition, retention, and dissemination of non-publicly available USPP information.

~~(U//FOUO)~~ In addition to targeting and minimization procedures, FAA §702 requires the Attorney General in consultation with the DNI, to adopt guidelines to ensure compliance with the limitations in the Act on acquisition of communications. These are documented in *Guidelines for the Acquisition of Foreign Intelligence Information Pursuant to the Foreign Intelligence Surveillance Act of 1978*. Approved by the Attorney General in 2008, the guidelines reinforce the targeting procedures established

<sup>45</sup> ~~(U//FOUO)~~ Acquisition is the collection by NSA or the FBI through electronic means of non-public communications to which they are not intended parties.

~~-TOP SECRET//SI//NOFORN-~~

ST-14-0002

requirements for application of the targeting procedures and establish requirements for obtaining court orders.

(U//~~FOUO~~) The government's FAA §702 certifications, targeting procedures and minimization procedures (but not the Attorney General Guidelines) require FISC approval. The FAA §702 certifications are accompanied by affidavits from the heads of elements of the IC, such as the DIRNSA, that describe the Agency's basis for assessing that acquisition will be consistent with statutory authorization and limits.

### **(U) Methodology and Scope**

---

(U//~~FOUO~~) Our review of the FAA §702 control framework, incidents of non-compliance, and NSA's use of the authority to support its mission, was based largely on FAA §702 stakeholder interviews and reviews of policies, procedures, and other program documentation. The OIG's *Special Study: Assessment of Management Controls Over FAA §702*, revised and reissued 29 March 2013, was also used as a resource. That study examined the controls designed to ensure compliance with FAA §702 and the targeting and minimization procedures associated with the 2011 certifications. Given the time constraints for the current review and the agreement with staff of the Senate Committee on the Judiciary, we did not verify through testing that all controls were operating as described by FAA §702 program stakeholders.<sup>46</sup>

(U//~~FOUO~~) Our review focused on the processes and documents implemented in 2013. Two documents filed annually with each FAA §702 certification delineate NSA's procedures for complying with the FISA Amendments Act of 2008:

- (U//~~FOUO~~) *Procedures Used by the National Security Agency for Targeting Non-United States Persons Reasonably Believed to be Located Outside the United States to Acquire Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended* (FAA §702 Targeting Procedures) and
- (U) *Minimization Procedures Used by the National Security Agency in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended* (the FAA §702 Minimization Procedures).

(U//~~FOUO~~) For calendar year 2013, the period under review, different versions of these documents were in effect because of changes made at the annual certification renewal and special amendments to the procedures.

- (U) Targeting Procedures
  - (S//NF) Procedures approved with the 2012 renewal of the authority, effective 24 September 2012 through 10 September 2013.

<sup>46</sup> (U//~~FOUO~~) The NSA OIG has conducted several audits and special studies on the effectiveness of certain FAA §702 program controls.

~~-TOP SECRET//SI//NOFORN-~~

- o (S//NF) These procedures were not changed for the 2013 certification renewal and remained effective 10 September 2013 through 28 August 2014.

- (U) Minimization Procedures

(b)(1)  
(b)(3)-P.L. 86-36

- o (S//NF) Procedures approved for the 2012 certification renewal, approved by the FISC 24 August 2012, were effective 24 September 2012 through 23 September 2013.

(b)(1)Hf

(b)(3)-P.L. 86-36  
(b)(3)-50 USC 3024(i)



- o (U//FOUO) An amended version of the 2013 minimization procedures approved 13 November 2013, added special procedures for assessing NSA's ability to use collection received when NSA's [REDACTED] Post-tasking checks were not functioning properly and procedures for handling data collected during a period in 2013 when these checks were not performing as intended.

(U) We also examined implementing procedures and controls for the Attorney General's targeting guidelines.

## **(U) FAA §702 Program Control Framework**

(U//FOUO) The FAA §702 control framework describes how NSA targets, collects, retains, accesses, processes, disseminates, and disengages FAA §702 data and the oversight mechanisms to comply with FAAA §702 certifications, including FISC-approved targeting and minimization procedures. This section summarizes the provisions of the targeting and minimization procedures and the controls implemented for each phase of the FAA §702 production cycle.

### **(U) Targeting**

#### **(U) Provisions of FAA §702 certifications**

(S//NF) The FAAA §702 targeting procedures set forth the measures that NSA uses to determine whether a prospective target is eligible for targeting under this authority. Each prospective target must meet three criteria. The individual must be a non-USP, reasonably believed to be located outside the United States, who possesses or is likely

<sup>47</sup> (U) A target is a person or entity against which intelligence operations are conducted. Foreign intelligence is obtained by tasking the target's selectors (e.g., e-mail addresses) to acquire information pursuant to one of NSA's authorities.

~~TOP SECRET//SI//NOFORN~~

ST-14-0002

to communicate foreign intelligence information consistent with one of the [D] FAA §702 certifications.<sup>48</sup>

(S//NF) The targeting procedures state that, when NSA proposes to direct surveillance at a prospective target, it does so only after it has learned something about the prospective target or the facilities the individual uses to communicate. For example, NSA personnel may examine lead information, obtained from a non-NSA element, such as tips from the CIA or FBI. [ ] P9

(b)(1)

(b)(3)-P.L. 86-36

(b)(3)-50 USC 3024(i) (S//NF) NSA personnel must also assess whether the prospective target possesses or is likely to communicate foreign intelligence information concerning foreign power [ ] and whether the proposed target is appropriate under one of the [ ] FAA §702 certifications.

(b)(3)-P.L. 86-36

#### **(U) Targeting process overview**

(U//FOUO) To initiate targeting under FAA §702 authority, NSA personnel must research the prospective target to determine whether it meets the requirements of this authority and to identify selectors that will yield communications from the prospective target.<sup>50</sup> Mission analysts operate within an assigned mission team (see the Access and Training section) and follow targeting guidance established by SID Analysis and Production on the basis of the FAA §702 Targeting Procedures to complete the analysis that forms the basis for a targeting request (TR). The [ ] is the vehicle for development and submission of TRs, [ ]

The TR documents information supporting the targeting decision and is subject to at least two levels of review before targeting. Additional reviews may be performed by the SID Data Acquisition (\$3) office of Targeting Strategy and Mission Integration (TSMI) and SW.

(U//FOUO) Mission analysts are responsible for the initial research and identification of potential targets within their organization's assigned missions. Analysts must complete a training regimen involving general courses on legal authorities and annual courses on FAA §702 procedures to be eligible to submit TRs under this authority and access and handle FAA §702 data (see the Access and Training section).

#### **(U) Provisions of FAA §702 certifications—eligibility for targeting**

(S//NF) **Foreignness determination** The targeting procedures require that NSA personnel examine, as appropriate under the circumstances, three categories of information to determine whether the intended target is not reasonably believed to be outside the United States (the foreignness determination). The

<sup>48</sup> (U) FAA does not define the term "reasonable belief," but the Act requires that NSA adopt targeting procedures to ensure that FAA §702 acquisition is limited to targets reasonably believed to be outside the United States.

<sup>49</sup> (U) Facilities are communication vehicles used by targets, including telephone numbers and e-mail addresses. NSA tasks these facilities or "selectors" to obtain foreign intelligence from approved targets.

<sup>50</sup> (U) Selectors are unique identifiers of targets (entities against which intelligence operations are conducted), such as telephone numbers and e-mail addresses, used for tasking (initiating SIGINT collection for the target's selectors).

~~TOP SECRET//SI//NOFORN~~

determination is based on the totality of information available about the prospective target's location and status as a USP and may be obtained from any one or a combination of these sources:

- (S//INF) [REDACTED]
- (b)(1) (b)(3)-P.L. 86-36 [REDACTED]
- (S//INF) [REDACTED] ,  
~1 :::::-r=====,1
- (S//INF) [REDACTED]  
-1 [REDACTED]

(U//FOUO) **Foreign intelligence purposes for targeting** In addition to the foreignness determination, NSIA personnel must assess whether the prospective target possesses, is expected to receive, and/or is likely to communicate foreign intelligence pursuant to one of the FAA §702 certifications.<sup>51</sup> Each certification identifies categories of foreign intelligence (see **Background** at the beginning of FAA §702 section) and specifies activities for which foreign intelligence collection is approved.

(S//NF) Targeting must also comply with the *Attorney General's Guidelines for the Acquisition of Foreign Intelligence Information Pursuant to the Foreign Intelligence Surveillance Act of 1978*, which reiterates the five targeting activities prohibited by FAA §702:

- (U) Intentionally targeting a person known at the time of acquisition to be in the United States;
- (U) Reverse targeting that is, targeting a non-USP outside the United States for the purpose of targeting a particular, known person reasonably believed to be in the United States;
- (S//NF) Intentionally targeting a USP reasonably believed to be outside the United States;
- (U) Intentionally acquiring communications as to which the sender and all intended recipients are known at the time of acquisition to be in the United States; and
- (U) Targeting inconsistent with the Fourth Amendment to the Constitution of the United States.

---

<sup>51</sup> (U) Foreign intelligence information is defined in FISA as (1) information that relates to, and if concerning a USP is necessary to, the ability of the United States to protect against- (A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power; (B) sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power; or (C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or (2) information with respect to a foreign power or foreign territory that relates to, and if concerning a U.S. person, is necessary to- (A) the national defense or the security of the United States or; (B) the conduct of the foreign affairs of the United States.

-TOP SECRET//SI//NOFORN-

ST-14-0002

(U) Targeting control procedures

(S//NF) Target research-forigness [redacted]

(b)(1) P  
(b)(3)-P.L. 86-36

(U//FOUO) **Target research-forign intelligence determination** NSA mission analysts task targets that are aligned with the National Intelligence Priorities Framework, can be linked to one of the foreign intelligence purposes specified in the appropriate FAA §702 certification and, generally, are within the analysts' assigned mission areas.<sup>52</sup> [redacted]

(b)(3)-P.L. 86-36

(U//FOUO) **Targeting request** Once mission analysts complete the research for the proposed target, they must develop and submit a TR [redacted] identified for an eligible target. The TR documents the analyst's determinations that the prospective target meets the standards in the targeting procedures. Once the TR has been reviewed and approved (see Targeting Authorization), the selected identifier in the TR is used to initiate collection. To complete a valid TR, mission analysts must compile specific information to demonstrate that, based on the totality of the circumstances determined from the search performed, the seal is reasonable belief that the proposed target is foreign (not a USP and not within the United States) and is likely to produce foreign intelligence consistent with one of the FAA §702 certifications. The TR must include:

<sup>52</sup> (U//FOUO) Raw data is data that has not been evaluated for foreign intelligence or processed to handle USP identities pursuant to the minimization procedures. Metadata is dialing, routing, addressing, or signalling information associated with communication but does not include information concerning the substance of the communication.

<sup>53</sup> (U) The National Intelligence Priorities Framework translates national foreign intelligence objectives and priorities approved by the President into specific prioritization guidance for the IC. It serves as guidance for U.S. foreign intelligence analysis and collection.

-TOP SECRET//SI//NOFORN-

~~TOP SECRET//SI//NOFORN~~

ST-14-00002

- (U//FOUO) [REDACTED]
- (U//FOUO) [REDACTED]
- (U) Sources supporting the determination of foreignness.<sup>54</sup>

(b)(3)P.L.86-36

(U//FOUO) Mission analysts must create permanent documentation of the information sources used to establish foreignness. Copies of the source information are saved in a restricted access SharePoint site SV maintains. This repository facilitates approval of the TR, as well as internal and external oversight.

(U//FOUO) The [REDACTED] system supports targeting compliance as the mission analyst creates the TRR. The system requires:

(b)(3)P.L.86-36

- (S//REL TO USA, PVIEW) Detailed information establishing the foreignness of the selector. [REDACTED]
- (U//FOUO) Target information, including the TRR,
- (U//FOUO) Completion of key fields to document information about the prospective target (e.g. authorized targeting purpose how the individual was determined to be outside the United States, basis for expectation that targeting the individual will produce foreign intelligence) and
- (U) Identification of the appropriate FAAA §§702 certification.

(b)(f)

(b)(3)P.L.86-36

(b)(3)-50 USE 3024(i)

(U//FOUO) The [REDACTED] system also:

(b)(3)P.L.86-36

(b)(1)

(b)(3)P.L.86-36

- (U) Identifies conflicting data within the TR,
- (U) Captures references to supporting documentation,
- (S//REL TO USA, PVIEW) [REDACTED]
- (S//REL TO USA, PVIEW) [REDACTED]

<sup>54</sup> (U) Targeting Rationale is a brief justification for targeting a selector, intended to explain the connection between the proposed target and a foreign intelligence purpose.

<sup>55</sup> (S//REL TO USA, PVIEW) [REDACTED]

~~-TOP SECRET//SI//NOFORN-~~

ST-14-0002

(b)(1)  
(b)(3)-P.L. 86-36

(S//NF)

(b)(1)  
(b)(3)-P.L. 86-36  
(b)(3)-50 USC 3024(i))

(S//NF) ~~~~~

(TS//SI//REL TO USA, FVEY)

(b)(1)...  
(b)(3)-P.L. 86-36  
(b)(3)-50 USC 3024(i))

(TS//SI//NF)

~~-TOP SECRET//SI//NOFORN-~~

(b)(1)  
(b)(3)-P.L. 86-36  
(b)(3)-50 USC 3024(i)

(TS//SI//NF)

1

- (U//FOUO) [REDACTED] (b)(3)-P.L. 86-36
- (U//FOUO) [REDACTED]
- (S//NF) [REDACTED] (b)(1)  
(b)(3)-P.L. 86-36  
(b)(3)-50 USC 3024(i)

(TS//SI//NF)

(b)(1)  
(b)(3)-P.L. 86-36  
(b)(3)-50 USC 3024(i)

(TS//SI//REL TO USA, P.R.Y.)

**(U) Provisions of FAA §702 certification and authorization to target**

(U//FOUO) Approval to task a prospective target's selector requires that the TR entry for that tasking be reviewed to verify that it contains the necessary citations to source information that led the analyst to reasonably believe that the individual is a

~~TOP SECRET//SI//NOFORN~~

ST-14-0002

non-USP outside the United States and is linked to the appropriate FAA §702 certification.

**(U) Targeting authorization controls**

**(U//FOUO)** NSA has implemented a multi-level review process to approve all proposed targeting.

**(U//FOUO) Releaser review** Submitted TRs are first reviewed by the mission releaser. Normally, the releaser is in the same organization as the mission analyst. Releasers must complete the same training courses as mission analysts. They examine the TRs for completeness and compliance with the FAA §702 Targeting Review Guidance developed and maintained by the Mission and Compliance staff, part of the Directorate for Analysis and Production, within NSA's Signals Intelligence Directorate.<sup>58</sup>

**(U//FOUO) Adjudication** [REDACTED] the final approval of the TR, known as adjudication, is a critical control point in tasking selectors under FAA §702 authority and is performed by personnel designated as mission adjudicators. TRs were initially subject to adjudication by SV but, [REDACTED]

(b)(3)-P.L. 88-36

[REDACTED] the responsibility was moved to the mission groups within the SIGINT Analysis and Production organization, where specially trained and experienced analysts, usually from the same organization as the targeting analyst, perform adjudication.<sup>59</sup> Adjudicators must complete the same courses as other mission personnel as a prerequisite for access to FAA §702 data (see the Access and Training section). They must also complete a specific course on adjudication and receive on-the-job training in their mission office before they are permitted to adjudicate independently. Adjudicators receive advice and updated information from the staff of the SIGINT Analysis and Production organization, SV, and OGC on developments affecting the application of the FAA §702 authority. The majority of adjudicators have two or more years experience in adjudication. Adjudicator performance is monitored by the Mission and Compliance staff in SID's Directorate for Analysis and Production.

**(CNREL TO USA, FVEY)** Adjudicators review TRs for accuracy, evaluate the evidence in the TR supporting the foreignness of the proposed target, examine the TAR statement for the individual's foreign intelligence value, and verify that the TR supports eligibility for targeting under the specified FAA §702 certification. As part of their TR reviews, adjudicators recreate the steps taken by the mission analyst to independently confirm that the supporting data is accurate and that the most current information available is used to support a reasonable belief that the prospective target

<sup>58</sup> **(U//FOUO)** As part of the Operations Staff for the S2, the staff includes teams who provide support and oversight of SID's use of FAA §702, such as [REDACTED] (S203-A U) and [REDACTED] (S203A7).

<sup>59</sup>~~TOP SECRET//SI//NOFORN~~

TOP SECRET//SI//NOFORN

ST-14-0002

is foreign. Following this same procedure, mission analysts and adjudicators [REDACTED]

(b)(1)

(b)(3)-P.L. 86-366

[REDACTED] to determine whether there is supporting or contrary information regarding the foreignness of the individual. Adjudicators must complete a series of checks manually or assisted by technology:

(b)(3)-P.L. 86-366

- (U//FOUO) [REDACTED], for an initial foreignness determination.<sup>60</sup>

- (TS//SI//REL TO USA, FVEY) Reviewing the databases of selectors

[REDACTED] 1 [REDACTED] 4 [REDACTED]

[REDACTED] whether there was information indicating that the

individual was not foreign.

- (U//FOUO) Accessing the SV4 SharePoint Site to determine whether there is information that would prohibit the current tasking request from being approved.

- (U//FOUO) [REDACTED]

[REDACTED] L [REDACTED]

(U//FOUO) If adjudicators are able to confirm that the prospective target meets the FAA §702 requirements for tasking, they approve the target's selector for tasking [REDACTED]

[REDACTED] However, if there is an error or required information is absent in the TR, adjudicators must ensure that corrective action is taken before approving the TR.

(TS//SI//REL TO USA, FVEY) In most instances, if adjudicators identify updated foreignness information, they substitute that information in the TR to ensure that the TR is current. If adjudicators find an error, such as inaccurate foreignness information, insufficient evidence to support foreignness, or an incomplete TAR statement, adjudicators may deny the TR and return it to mission analysts for correction. When the TR is corrected, the TR goes back to the mission manager and the mission adjudicator. As part of the approval process, adjudicators upload documentation of the sources supporting the targeting decision onto the SharePoint site that SV maintains.

(TS//SI//REL TO USA, FVEY)

TOP SECRET//SI//NOFORN

~~TOP SECRET//SI//NOFORN~~

ST-114-0002

(b)(3)-P.L.866386

(U//~~FOUO~~) The targeting review process is summarized in Figure 8.

**(U) Figure 8. FAA §702 Targeting Review Process**



**(U) Provisions of FAA §702 certifications/approval of TRs from other agencies**

(U//~~FOUO~~) The FAA §702 minimization procedures set forth processes NSA uses for the acquisition, retention, use, and dissemination of information acquired under FAA §702.

(U//FOUO) In accordance with Section 16(e) of the minimization procedures, NSSA provides the CIA and the FBI unminimized communications acquired pursuant to FAA § 702 for targets nominated by the respective agencies and approved for tasking in accordance with NSSA's targeting procedures.

Both the CIA and the FBI must handle unminimized communications received from NSA in accordance with their FISC-approved minimization procedures adopted by the Attorney General in consultation with the ODNI.

(b)(3)-P.L.866386

(b)(3)-P.L.866366

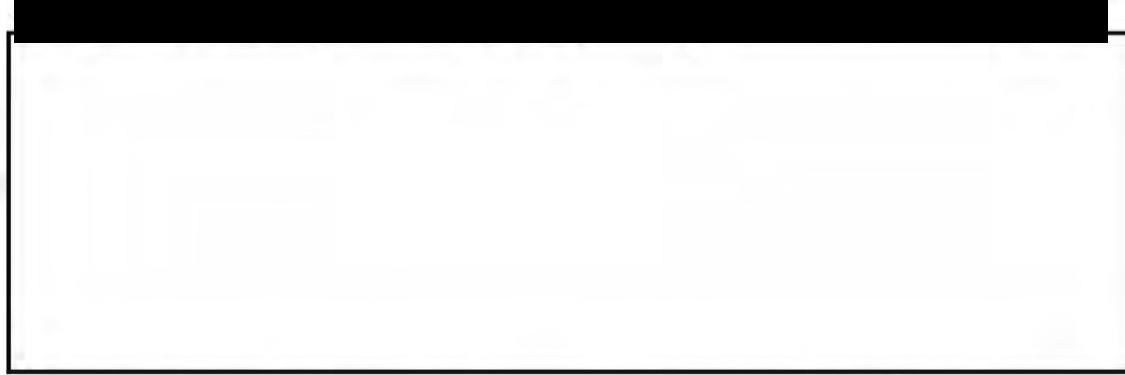
~~TOP SECRET//SI//NOFORN~~

TOP SECRET//SI//NOFORN

ST-14-0002

## (U//FOUO) Contracts over approval of CIA and FBI TRs

(S//REL TO USA, FVEY) The CIA and the FBI submit requests of tasking selectors of prospective targets to NSA, which reviews the foreignness information and the foreignness justification for the prospective target and approves these selectors for tasking upon an assessment that there is a reasonable belief that the prospective target is a non-USP outside the United States and that collection will produce foreign intelligence information pursuant to one of the approved certifications.

(b)(1)

(b)(3)-P.L. 86-36

(U//FOUO) Table 26 summarizes the targeting provisions of the FAA §702 targeting procedures and the controls NSA has implemented to maintain compliance.

## (U) Table 26. Targeting Provisions and Controls

(TCS//SI//NF)

| Provision   | Control  |
|---|--|
| (U) Foreignness -- Acquisition targets only non-USPs reasonably believed to be outside the United States<br><br>(b)(1)<br>(b)(3)-P.L. 86-36 | (U//FOUO) The TIR documents the support for NSA's determination of the prospective target's foreignness.<br>(TCS//SI//REL TO USA, FVEY) The targeting system [C=J] enforces completion of required fields (including foreignness information), identifies conflicting data, flags selectors ineligible for tasking.<br><br>[redacted] and captures source information supporting targeting.<br>(U//FOUO) All TRs are subject to at least two levels of review prior to targeting. Additional reviews may be performed by TSIM or SV. Reviewers examine available information to validate accuracy of the foreignness determination and that conflicting information has been resolved. |

(b)(3)-P.L.

<sup>63</sup> (U) An MCT is an Internet "transaction" that contains more than one discrete communication within it. If one of the communications within an MCT references a tasked selector and one end of the transaction is foreign, the entire MCT transaction will be acquired through upstream Internet collection techniques. Since this can include discrete communications that do not contain the tasked selector, use of such information must meet specific requirements.

TOP SECRET//SI//NOFORN

~~-TOP SECRET//SI//NOFORN~~

ST-14-0002

|  |   |
|--|---|
| (b)(1)<br>(b)(3)-P.L. 86-36<br>(b)(3)-50 USC 3024(i)   | (TS//SI//REL TO USA, FVEY)<br><br>(TS//SI//REL TO USA, FVEY)<br><br>(TS//SI//REL TO USA, FVEY)  |
| (S//SI//NF) NSA will maintain records of selectors [REDACTED]  | (S//SI//NF) NSA maintains these records in a database of selectors* [REDACTED] This tool is used in target research by analysts and interfaces with [REDACTED] to identify ineligible selectors proposed for targeting. The information generated is reviewed by the adjudicators and any conflicts should be resolved before the TRs are approved. (b)(3)-P.L. 86-36 |
| (U) Foreign Intelligence Purpose of Targeting - NSA will assess whether the target possesses or is likely to communicate foreign intelligence pursuant to one of the approved certifications.                      | (U//FOUO) The TRS statement documents why targeting is requested and indicates the foreign intelligence purpose specific to the FAAA Certification under which targeting is requested. This is subject to adjudication.   |
| (U) NSA may provide unminimized communications acquired pursuant to FAA §702 to the CIA and FBI.   | (S//REL TO USA, FVEY) The CIA and FBI may nominate targets and selectors for acquisition, subject to NSA's targeting procedures. (b)(1)<br>(b)(3)-P.L. 86-36<br><br>The CIA and FBI have their own minimization procedures for processing the unminimized data that they receive.   |
| (U//FOUO) Tasking requests must be supported by citations to the information that led to the analyst's reasonable belief of the foreignness of the target. Approval of the TR will include review of the citation. | (U//FOUO) The adjudication review includes examination of the citations supporting the foreignness determination maintained in the SV SharePoint site.  |

(TS//SI//NF)

**(U) Provisions of FAA §702 Certifications and other Guidance—Post-Targeting Review**

(S//NF) In accordance with the targeting procedures set forth in each FAAA §702 certification, NSA analysts are required to conduct post-targeting reviews of all selectors tasking under FAAA §702 authority. The targeting procedures state that "Such analysis is designed to detect those occasions when a person who when targeted, was reasonably believed to be located outside the United States has since entered the United States, and will enable NSA to take steps to prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of acquisition to be located in the United States, or the intentional targeting of a person who is inside the United States."

~~-TOP SECRET//SI//NOFORN~~

## (U) Post-targeting

(S//NF) NSA has implemented four procedures to ensure that targeted persons continue to meet the criteria specified in the FAA §702 targeting procedures.

(S//REL TO USA, FVEY) Post-targeting controls obligation to review NSA has implemented a process called Obligation to Review (OtR) that has two provisions. The first requires that, upon tasking a selector, the mission team that initiated the tasking must review collection from that tasking within 5 business days of the receipt of the initial piece of traffic from FAA §702 collection. An e-mail notification is sent to mission team members notifying them of the receipt and the 5 day review requirement. The mission analyst must review sample of the content of the collection to determine that:

- (U) The selector is being used by the intended target,
- (U) The target is valid under the requested FAA §702 certification, and
- (S//REL TO USA, FVEY) [REDACTED]

1

(U//FOUO) If the reviewing analyst determines that all three requirements have been satisfied, thus making the tasking valid under FAA §702 authority, no further action is required. If any of the three requirements is not satisfied, the selector must be immediately detasked in the [REDACTED] system (removed from collection). The selector cannot be resubmitted for tasking until all requirements have been satisfied.

(Detasking is discussed further in Monitoring Collection section.)

(b)(3)-P.L. 86-36

(U//FOUO) The second provision of the OtR process requires the mission office to conduct an ongoing review of at least a sample of the content from ongoing collection to ensure that the target continues to meet the criteria for targeting under FAA §702. After the initial review has been completed, a sample of collection is reviewed [REDACTED]

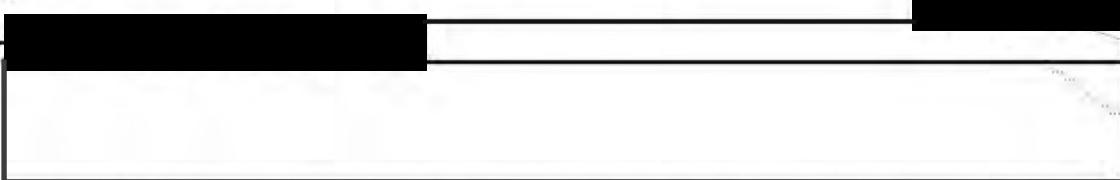
(S//REL TO USA, FVEY)

(S//REL TO USA, FVEY)

(b)(1)  
(b)(3)-P.L. 86-36

~~TOP SECRET//SI//NOFORN~~

ST-14-0002



**(U//FOUO) Post-targeting controls-monitoring collection** Mission analysts must monitor collection if indications that the target no longer meets the foreignness requirements, is not associated with the tasked selector, or is not linked to a valid foreign intelligence purpose tied to an FAA §702 certification. If it is determined that the target or the selector is no longer appropriate for tasking under this authority, NSA will have to take actions that might include detasking the selector, preparing a compliance incident, recalling intelligence reports, and purging collected communications.

**(U//FOUO)** If collection indicates [REDACTED] user of a tasked selector is an individual who is not the intended target and is not of foreign intelligence value or is or may be a USP or is in the United States, the mission office must immediately remove from collection all selectors [REDACTED] and identify collection ineligible for retention. Additional research may be performed before detasking, if there is evidence that the information on the user's USPs status or location is not correct. Unless there is a strong reason to doubt this information from collection, it is presumed valid and detasking should occur immediately. If review of collection identifies communications in which the selector and all identified recipients are determined to have been within the United States at the time of collection (domestic communications), those communications must be destroyed with limited exceptions.<sup>64</sup>

**(U)** If analysis of the collection finds that the selector is no longer used by the target, the selector must be removed from tasking.<sup>65</sup>

**(U//FOUO)** Attorney-client privileged communications are subject to special procedures designed to prevent privileged information from being used in prosecution. Should review of collection identify communications between persons known to be under criminal indictment in the United States and their attorneys, review of the communication must be discontinued and OGC notified for guidance on handling the communication.<sup>66</sup>

<sup>64</sup> **(U//FOUO)** If the domestic communication collected is not related to an incident (see Incident Reporting) DIRNSA may approve a destruction waiver to allow retention of the collection.

<sup>65</sup> **(S//SI//REL TO USA, FVEY)** [REDACTED]

**(SffSIHREL : : ~ ~ m v)** [REDACTED]

<sup>66</sup> **(U//FOUO)** Monitoring communications between a person known to be under criminal indictment in the United States and an attorney representing that individual in the matter under indictment must cease once the relationship has been identified. The acquired communications must be logged and NSD notified so that measures may be taken to protect such communications from review or use in criminal prosecutions.

~~TOP SECRET//SI//NOFORN~~

~~TOP SECRET//SI//NOFORN~~

ST-14-0002

(U//~~FOUO~~) If authorized collection incidentally acquires foreign communication of or concerning a USP (e.g., an FAA §702 target is communicating with a USP or about a USP), the communication may in general only be retained if the USP information qualifies as foreign intelligence or the information is evidence of a crime and is provided to appropriate federal law enforcement authorities. Domestic communications, including communication of a target who has entered the United States, must in general, be destroyed upon recognition unless DIRNSA or the Acting DIRNSA approves retention of the communication for one of the limited reasons listed in Section 55 of NSA's FAA §702 minimization procedures. (b)(3)-P.L. 86-36

(U//~~FOUO~~) For intelligence collected from upstream Internet collection [ ] subject to MCTs, NSA mission analysts must identify and carefully review collection containing MCTs made available for analytic review. While NSA automatically segregates certain MCTs and does not pass them to repositories accessible to analysts, there may still be information in some MCTs that is not eligible for retention. If a discrete communication within an MCT is not to, from, or about attackable selector but otherwise contains foreign intelligence information and the discrete communication is not to or from an identifiable USP or a person reasonably believed to be in the United States, the MCT may be retained to the same degree that a discrete communication could be retained. If any portion of the MCT contains a domestic communication the entire MCT must be purged, unless there is no underlying compliance incident and DIRNSA approves a classification waiver.

(U) For selectors removed from tasking, all communications collected after the target no longer meets the requirements of FAA §702 must be identified for purging through incident reporting and the purge adjudication process (see the Purge section).

~~(TS//SI//NF) Post-targeting controls detection of targets that may have entered the United States~~ [ ] In addition to analyst review of

(b)(1)  
(b)(3)-P.L. 86-36  
(b)(3)-50 USC 3024(i)

selector communications, NSA has implemented [ ] for indications that the user of a tasked selector has entered the United States [ ]

[ ] immediately detasks the ongoing selector and [ ] sends a message to mission analysts notifying them that the selector has been de tasked. It is the analysts' responsibility to identify and de task additional selectors for the target and develop the information necessary to produce an incident report. Though NSA may not have had prior notice of the target's intention to travel, FAA §702 may not be used to target individuals in the United States (see the Incident Reporting section). (b)(3)-P.L. 86

~~(S/REL TO USA, FVEY)~~ [ ]

[ ] ----- ~

~~TOP SECRET//SI//NOFORN~~

-TOP SECRET//SI//NOFORN-

ST-14-0002

(b)(1)  
 (b)(3)-P.L. 86-36  
 (b)(3)-50 USC 3024(i)

(S//REL TO USA, FVEY)

(b)(1)f  
 (b)(1)  
 (b)(3)-P.L. 86-36

(U//FOUO) Post-targeting controls periodic selector review As discussed earlier, NSA is required to regularly confirm that all selectors tasked under FAA §702 continue to meet targeting requirements. In addition to these ongoing reviews, [REDACTED] defaults all FAAA §702 targeting to a one year review. To maintain acquisition for the target, mission analysts must confirm that continued tasking of the selector is expected to acquire foreign intelligence relevant to the FAA §702 certification under which the targeting was executed.

(b)(3)-P.L. 86-36

(U//FOUO) Table 27 summarizes the post-targeting provisions of the FAA §702 targeting procedures and the controls implemented by NSA to maintain compliance.

**(U) Table 27. Post-Targeting Provisions and Controls**

(S//SI//NF)

| Provision   | Control  |
|---|--|
| (U//FOUO) Post-targeting analysis is performed to detect when a person, reasonably believed to be outside the United States when targeted, has since entered the United States. This will allow NSA to take steps designed to prevent acquisition of domestic communications or the targeting of a USP. | (U) Analysts are required to monitor collection to determine whether the target continues to meet targeting criteria, including foreignness.<br>(U) Analysts receive "obligation to review" notices upon first receipt of collection for newly tasked Internet selectors and every thirty days commencing with the date of first collection after the last review. The notice is repeated until collection has been reviewed.<br>(U) Annual reviews confirm that a target remains eligible for targeting and continues to be expected to produce foreign intelligence relevant to the FAAA §702 certification under which it was approved. |
| (S//SI//REL TO USA, FVEY)<br>NSA will routinely compare tasked selectors with information collected from  | (S//REL TO USA, FVEY)  |

67 (TS//SI//REL TO USA, FVEY)

-TOP SECRET//SI//NOFORN-

TOP SECRET//SI//NOFORN

ST-14-0002

(b)(f)  
 (b)(3)-P.L. 86-36  
 (b)(3)-50 USC 3024(i)

|   |   |
|---|---|
|   | or detasking of the selector and purge of any non-compliant communications.   |
| (S//SI//NF) NSA will routinely compare selectors tasked   | (S//REL TO USA, FVEY) See Table 26 - second control.  |
| (S//SI//NF) NSA will [redacted] for indications that a foreign target has entered or intends to enter the United States.  | (U) Automated notices are sent to mission teams upon first receipt of collection from newly tasked Internet selectors and every thirty days commencing with the date of first collection after the last review. The notice is repeated until collection has been reviewed.<br><br>(b)(3)-P.L. 86-36   |
| (U) If NSA determines that a target has entered the United States, it will take the necessary steps to assess whether the incident represents non-compliance with the targeting procedures and report such occurrences to DoJ and ODNI and purge related communications from NSA databases as required.   | (U) See the Incident Recognition and Reporting section.<br>(U) If NSA determines that a target has entered the United States and the target's selectors were not detasked before entry, it is reported to DoJ and ODNI as an incident. DoJ assesses which incidents represent non-compliance with the targeting procedures and reports such occurrences to the FISC. NSA purges related communications from NSA databases as required. In some cases, DIRNSA may gain habeas protection in NSA against collection that is otherwise subject to purge. |
| (U) If NSA determines that a target who at the time of targeting, was believed to be a non-USP is in fact a USP, it will terminate collection without delay and report the incident to DoJ and ODNI and purge such collection from its databases.   | (U) See the Incident Recognition and Reporting section.   |
| (U//FOUO) As soon as it becomes apparent that a communication is between a person who is known to be under criminal indictment in the United States and an attorney who represents that individual in the matter under indictment, monitoring of that communication will cease and the communication will be identified as an attorney-client communication in a log maintained for that purpose. | (U//FOUO) Annual FAA training requires that such communications be brought immediately to OGC's attention for further instruction. OGC maintains e-mail records of such communications. [redacted] DoJ has agreed that the process used to quarantine these communications is a sufficient process for documenting the information.<br><br>(b)(3)-P.L. 86-36  |

(S//SI//NF)

### (U) Incident Recognition and Reporting

#### (U) Provisions of FAA §702 certifications—incident reporting

(U//FOUO) The targeting procedures statethat NSA will conduct ongoing oversight and report incidents offnon-compliance to the NSA OIG and OGC and ensure that corrective actions are taken to address deficiencies. Reporting is required for incidents of non-compliance “that result in the intentional targeting of a person

TOP SECRET//SI//NOFORN

~~TOP SECRET//SI//NOFORN~~

ST-14-0002

reasonably believed to be located in the United States, the intentional targeting of a USP, or the intentional acquisition of any communication in which the sender and all intended recipients are known at the time of acquisition to be located within the United States." NSA must report these incidents within five business days of discovering about them. The Agency must purge from its databases information acquired by intentionally targeting a USP or a person or entity believed to be outside the United States at the time of targeting. If post-targeting analysis shows that the target is inside the United States or a USP, acquisition must be terminated without delay. Inadvertent acquisition of domestic communications is addressed in the minimization procedures (see the ~~Procedures~~). NSA also reports incidents of non-compliance with the FAA §702 minimization procedures. Some examples include incomplete minimization of USP information, improper queries of raw data, and technical errors that affect systems controls over the data, such as retention beyond the required destruction date.

#### **(U) Incident reporting controls**

**(U//FOUO)** Training and management communications emphasize that each incident can occur at any point in the collection, targeting, dissemination, access, and retention of SIGINT communications and stress the importance of immediate reporting of instances of non-compliance. Individuals do not have to prove that the activity is noncompliant to report an incident. SV works with the mission team that reports the matter to develop an incident report with complete and accurate information. If the incident involves a system or a system's performance, TV involves all appropriate subject matter experts (including SID, SV, TID, and OGC) to assess the situation and evaluate its self-compliance and determine authority. OGC informs DDoJ and ODNI of incidents that may indicate non-compliance with FAA §702. DoJ, in coordination with ODNI, makes the final determination whether an incident is reportable to the FISC.

**(U//FOUO)** The OIG receives internal incident reports from SV and TV. Notices of non-compliance (NNB notices) that DDoJ files with the FISC are made available to the OIG. The OIG uses this information to develop the Intelligence Oversight Quarterly Report, which is prepared with OGC and sent to the President's Intelligence Oversight Board through DoD. The incidents and notices of non-compliance are also used as input to OIG inspections and intelligence oversight reviews.

**(U//FOUO)** The annual FAA §702 training required of all individuals handling information obtained under this authority addresses incident recognition, reporting, and processing. It defines two types of reportable events: incidents of non-compliance and changes in the target's status.

**(U//FOUO) Reportable compliance incident:** An FAA §702 compliance incident occurs when NSA violates FAA §702 statutory requirements or targeting and minimization procedures or has made materially inaccurate representations to the FISC or has otherwise performed in a manner inconsistent with previous representations to the FISC. For example, if NSA tasked a foreign intelligence target reasonably believed to be outside the United States at the time of tasking and later

~~TOP SECRET//SI//NOFORN~~

learned that the target planned to travel to the United States but did not task the selector before the target's entry into the United States, this would be reported as a compliance incident.

(U//~~FOUO~~) Reportable compliance incidents may also result from actions taken by communications service providers. For example, provider error could cause distribution to NSA of communications for selectors not tasked under FAA §702.

(U//~~FOUO~~) **Change in target status** After tasking selectors associated with a target that meets all requirements of the targeting procedures, NSA may identify information about the target that was not available when the targeting decision was made. This information may show that the target is a USP if it is located in the United States, making the target ineligible for targeting. These changes in target status, though not incidents of non-compliance, must be reported.

(U//~~FOUO~~) **Incident reporting and documentation** SV has a significant role in reporting incidents of non-compliance with FAA §702. SV developed an operating procedure that addresses the implementation of incident discovery and the actions SW personnel follow for each. There are three primary sources from which SV may identify incidents:

(b)(3)-P.L.86-866

- (U//~~FOUO~~) Detask notifications produced by OW when mission personnel remove selectors from collection. A detargeting reason is associated with each notification, some of which may indicate an incident, e.g., the user of the tasked selector has been identified as a USP,
- [REDACTED] targets that appear to have roamed into the [REDACTED]
- (U//~~FOUO~~) Communications of incidents reported by analysts, query reviewers, and others involved in processing or monitoring collection. This may include errors by communications service providers.

(S//SI//REL TO USA, FVEY) For each incident, SV works with personnel familiar with the occurrence to create a permanent record including significant detail about the incident and its resolution, for example the selector, the intended target, [REDACTED]

[REDACTED] method of incident discovery, detasking information, and dates of collection to be purged. SV creates an entry in the database of selectors associated with targets that have come into the United States, have been identified as USPs to identify selectors associated with targets identified as meeting certain criteria. [REDACTED] generates a notice to analysts entering TRs. This entry is required when incidents identify a target located in the United States [REDACTED] or a target identified as a USP.

(b)(3)-P.L.86-866

(U//~~FOUO~~) TV is responsible for overseeing the reporting and mitigation of incidents that affect TD personnel and systems. For each incident, information regarding the incident's root cause and mitigation is gathered and documented. There are four primary ways in which incidents in TD are discovered:

~~TOP SECRET//SI//NOFORN~~

ST-14-0002

- (U//~~FOUO~~) Technical personnel or analysts find data that is not protected, labeled, or transferred as expected,
- (U//~~FOUO~~) Audits of queries submitted by TD personnel are reported when they do not comply with the minimization procedures,
- (U//~~FOUO~~) Upon analysis of a system for TV certification, instances of potential non-compliance are reported, and
- (U//~~FOUO~~) Technical personnel self report incidents.

(U//~~FOUO~~) SV and TV provide the incident reports to OGC to assess whether the incident is a matter of non-compliance with the FAA §702 certifications and targeting and minimization procedures such as is reportable to NSA's overseers (see the Oversight section).

(U//~~FOUO~~) **Incident remediation** Several types of activities may be necessary to resolve compliance incidents or changes in its status, for example, tasking debtors, purging communications ineligible for retention, recalling disseminated reports based upon communications subject to purge, correcting system errors, and training. The actions taken are documented in the incident report and, if appropriate, the notice of non-compliance filed with the FISC. Depending on the magnitude of an incident of non-compliance (e.g., a system error affecting the functioning of targeting tools), the FISC may require supplemental reports on progress in correcting the matter. SV and OGC coordinate such reports with DoJ and ODNI.

(U//~~FOUO~~) Table 28 summarizes the incident reporting provisions of the FAA §702 targeting procedures and the controls implemented by NSA to maintain compliance. The provisions are documented in the oversight and compliance requirements in the targeting procedures.

**(U) Table 28. Incident Reporting Provisions and Controls**

(U//~~FOUO~~)

| Provision  | Control  |
|--|--|
| (U) NSA will conduct ongoing oversight activities and will make necessary reports, including those relating to incidents of non-compliance, to the NSA OIG and OGC.  | (U) FAA §702 training addresses incident identification, documentation, and the process for self-reporting.<br>(U// <del>FOUO</del> ) SV and TV document the incident with assistance of the individuals who identified the matter and provide the information to OGC for review. OGC, in turn, forwards the incident to DoJ and ODNI. |
| (U) NSA will ensure that necessary corrective actions are taken to address identified deficiencies.  | (U) The incident report documents measures taken to remediate the incident (e.g., tasking and purge of communications).  |
| (U// <del>FOUO</del> ) NSA will report to DoJ, NSD and ODNI incidents of non-compliance (including over collection) by electronic communications service providers within five business days after determining non-compliance. | (U// <del>FOUO</del> ) SV, TV, and OGC manage the incident reporting process to assure that initial reporting is performed within five business days of the identification of non-compliance.  |

(U//~~FOUO~~)~~TOP SECRET//SI//NOFORN~~

## (U) Collection

(U) NSA's FAA §702 minimization procedures require that collection of information by targeting non-USPs reasonably believed to be outside the United States be conducted in a manner designed, to the greatest extent feasible, to minimize the acquisition of information not relevant for the purpose under which the collection was authorized. Steps to assure that acquisition meets this requirement start with target research and approval and the determination that the proposed target satisfies the criteria for eligibility under FAA §702. NSA has incorporated additional measures in its collection process to comply with this limitation.

## (U) Collection mechanisms for FAA §702 communications

(U) NSA has two collection mechanisms for FAA §702. [REDACTED] (b)(3)-P.L. 86-36 communications are obtained by the FBI through compelled collection from USPs and include only communications to which a tasked selector is a party. For upstream Internet collection and telephony collection, the communications service providers who control the telecommunications infrastructure over which the communications travel are legally compelled to make available to NSA communications related to tasked selectors. Upstream collection of Internet-based selectors may include communications to or from the tasked selector, as well as communications in which the selector is referenced within an Internet transaction. The latter is called "abouts" collection because the communication is neither to nor from the tasked selector, but "about" the selector, i.e. the selector is contained within the communication. Communications acquired from telephony selectors are only to or from the tasked telephone number (i.e., "abouts" collection is not a factor).

## (U) Provisions of FAA §702 certifications-filters

(S//SI//NF) NSA's FAA §702 targeting procedures state that, [REDACTED]

(b)(4)L

(b)(3)-P.L. 86-36

[REDACTED] employ an Internet Protocol filter to ensure that the person from whom it seeks to obtain foreign intelligence information is located in a foreign country.

## (U) Collection controls for telephony and upstream Internet communications—communications not to or from the target

(TS//SI//NF)

(b)(1)  
 (b)(3)-P.L. 86-36  
 (b)(3)-50 USC 3022(i)

~~-TOP SECRET//SI//NOFORN-~~

ST-14-0002

[REDACTED]

The providers should deliver only communications meeting the criteria NSA.

**(b)(1) (U) Provisions of FAA §702 certifications-analysis of selector targeting status**

(b)(3)-P.L. 86-36 (SURREY USA, FVEY) NSA's FAA §702 targeting procedures set forth criteria (b)(3)-50 USC 3024(i) for initiating collection on a target. Once a target's selector has been placed on collection, the Agency continues to evaluate collection and use other tools to identify changes in the status or location of the target (e.g., change in USP status, such as information that the individual has been granted permanent resident status in the United States or information that the target is entering the United States). If these changes occur or it is determined that the target is no longer producing foreign intelligence, the selector is removed from collection. Changes in targeting status may be processed immediately upon identification in NSA systems [REDACTED]

This requires NSA to [REDACTED]

[REDACTED] - [REDACTED]

**(U) Collection controls verification that collection is for currently tasked targets**

(S//NF) For each source of collection, NSA employs processes to determine whether [REDACTED] (b)(1)

[REDACTED] are sending communication only for selectors currently tasked and authorized for collection. [REDACTED]

(b)(3)-P.L. 86-36

**(U//FOUO) Collection for telephony selectors** [REDACTED]

(b)(3)-P.L. 86-36

[REDACTED]

**(TS//SI//NF) Upstream collection for Internet-based selectors** [REDACTED]

[REDACTED]

[REDACTED]

(b)(1)  
 (b)(3)-P.L. 86-36  
 (b)(3)-50 USC 3024(i)

~~-TOP SECRET//SI//NOFORN-~~

(b)(1)r  
(b)(3)-P.L. 86-36  
(b)(3)-50 USC 3024(i)

(TS//SI//NF) A situation known as [REDACTED] can result in the unintended acquisition of non-target communications [REDACTED]

A [REDACTED] NSA implemented a verification process to address this situation that is another check performed before upstream Internet communications are forwarded to analysts accessible repository for processing: [REDACTED]

(TS//SI//NF)

(b)(1)  
(b)(3)-P.L. 86-36  
(b)(3)-50 USC 3024(i)

**(U) Provisions of FAA §702 certifications—upstream Internet transactions**

**(U) Background** Upstream Internet collection includes acquisition of two types of communications not present in downstream collection: “about” communications and “multiple communications transactions” (MCTs). “About” communications are those that are not to or from the target selector but whose content is included in the selector. For example, if a target’s e-mail address is within the body of the Internet communication between two individuals, the communication “about” the selector. An MCT is an Internet “transaction” that contains more than one discrete communication. If one of those discrete communications is to, from or about a tasked selector and if the active end of the transaction is foreign, the entire MCT transaction will be acquired through upstream Internet collection. This can include other discrete communications that do not contain the tasked selector. If the targeted selector is not the active user in the transaction, the MCT can include other discrete communications that do not contain the tasked selector.

**(U) Provisions** NSA’s FAA §702 minimization procedures require NSA to:

~~TOP SECRET//SI//NOFORN~~

ST-14-0002

take reasonable steps post-acquisition to identify and segregate through technical means Internet transactions that cannot be reasonably identified as containing single, discrete communications where: the active user of the transaction (i.e., the electronic communications account/address/identifier used to send or receive the Internet transaction to or from a service provider) is reasonably believed to be located in the United States; or the location of the active user is unknown.

(U//~~FOUO~~) Internet transactions that cannot be identified as meeting the above definition must be segregated and retained in an access-controlled repository from which transactions may not be moved, except for processing to render them intelligible, unless they are determined to contain discrete communications for which the sender and all intended recipients are reasonably believed to be in the United States. Any such transactions moved to data repositories accessible by analysts are required to be identified as having been previously segregated.<sup>68</sup> NSA's FAA §702 minimization procedures also specify that Internet transactions acquired through NSA's upstream Internet collection techniques on or before 31 October 2011 be destroyed upon recognition.

**(U) Upstream Internet collection controls multiple communication transactions**

(TS//SI//NF) Effective January 2012, NSA implemented a process for analyzing and processing upstream Internet collection to ensure that only MCTs should be withheld from analysis. This process applied to all upstream data that had been sequestered starting November 2011.<sup>69</sup> Three criteria are used to sort these communications and determine whether they would be withheld from use by analysts (segregated in a collection store) or sent to data stores accessible by analysts: the type of communication (discrete or MCT), the active user of the selector, and the location of the active user. The minimization procedures require that sequestered communications be accessible only to specially trained personnel to determine whether they may be authorized for use:

[REDACTED] As [REDACTED]  
 (b)(1) NSA reported to the FISC, all FAA §702 upstream Internet transactions acquired before November 2011, whether or not they were MCTs, were deleted. Additional controls are required when MCTs available to analysts are used, for example, to support reporting of foreign intelligence (see the Sharing and Dissemination section).

(b)(1)  
 (b)(3)P.L.86-36

<sup>68</sup> (TS//SI//NF) Though the minimization procedures permit NSA to pass previously segregated communication to repositories accessible to analysts, NSA has not done so.

<sup>69</sup> (S//SI//REL TO USA, FVEY) [REDACTED] the only FAA §702 data forwarded to analyst-accessible repositories was data [REDACTED] or where the target was the active user. The remainder was sequestered pending development of decision logic to assess MCTs. The data was also excluded from [REDACTED]

~~TOP SECRET//SI//NOFORN~~

~~TOP SECRET//SI//NOFORN~~

ST-14-0002

(U) Table 29 summarizes the collection provisions of the FAA §702 minimization procedures and the controls implemented by NSA to maintain compliance.

**(U) Table 29. Collection Provisions and Controls**

~~(U//FOUO)~~ (U//FOUO)

| Provision   | Control   |
|---|---|
| <p>(U) Acquisition of information by targeting non-USPs reasonably believed to be outside the United States will be conducted in a manner designed, to the greatest extent feasible, to minimize the acquisition of information not relevant to the purpose for which it was authorized.</p> <p>(b)(1)</p> <p>(b)(3)-P.L. 86-386</p> <p>(b)(3)-50 USC 1822(i)</p>       | <p>(U//FOUO) Targeting controls (see Table 26) are the first measures employed to limit collection of communications of targets that meet the requirements for the targeting procedures. The foreignness requirement is added to post-targeting analysis of communications to avoid minimization of collection of communications not authorized for acquisition (e.g., domestic communications).</p> <p>(S//SI//NF)</p> <p>(U//FOUO) L-1 ~ IT</p> <p>(b)(3)-P.L. 86-386</p> |
| <p>(U//FOUO) Acquisition of communications not from from the target will employ an Internet protocol filter.</p> <p>I</p>   | <p>(U//FOUO) Internet protocol filtering is performed on collection.</p> <p>To verify that at least one end of each transaction is foreign. Only transactions meeting this criterion should be delivered to NSA.</p> <p>(S//SI//NF)</p>   |
| <p>(U) NSA will take reasonable steps post-acquisition to identify and segregate through technical means Internet transactions that cannot be reasonably identified as containing single, discrete communications where the active user of the transaction is reasonably believed to be located in the United States or the location of the active user is unknown.</p> | <p>(U//FOUO) NSA has implemented procedures to analyze upstream Internet collection. Only discrete transactions and MCTs meeting certain criteria are made accessible to analysts.</p> <p>(~H3).P<br/>(b)(3)-P.L. 86-386</p>  |

(U//FOUO)

~~(S//SI//NF)~~

**(U) Repositories**

**(U) Provisions of FAA §702 certifications-repositories**

(U//FOUO) NSA's FAA §702 targeting procedures require that NSA establish processes for ensuring that raw traffic is labelled and stored only in authorized repositories and is accessible only to those who have had proper training (see the Access and Training section).

~~TOP SECRET//SI//NOFORN~~

~~TOP SECRET//SI//NOFORN~~

ST-14-0002

**(U) Control framework for access to FAA §702 repositories**

(U//~~FOUO~~) Several control procedures are employed to ensure that FAA §702 data is stored in repositories that meet standards for security and compliance and that access to the data is properly controlled. From the time of collection, data is processed through interim systems before it reaches the [redacted] approved source systems for FAA §702 reporting.<sup>70</sup> The remainder of this section describes four types of controls, focusing on their application to the [redacted]

(b)(3)-P.L.866365

- (U//~~FOUO~~) System security accreditation,
- (U//~~FOUO~~) System certification,
- (U//~~FOUO~~) Data flow management, and
- (U//~~FOUO~~) Data tagging.

**(U//~~FOUO~~) Approval for NSA systems to store and process FAA §702 data**

(U//~~FOUO~~) **Accreditation** TS is responsible for managing the risks to all NSA networks and the computer systems and devices connected to those networks. TSS's responsibilities include:

- (U//~~FOUO~~) Guiding, prioritizing and overseeing the development of information assurance programs necessary to ensure protection of information systems and networks by managing the NSA Information Security Program,
- (U//~~FOUO~~) Serving as the Director NSA Authorizing Official to accredit all NSA information systems,
- (U//~~FOUO~~) Conducting information system security and accreditation and risk management programs, and
- (U//~~FOUO~~) Establishing, maintaining and enforcing NSA information systems security policies and implementation guidelines.

(U) Accreditation is the official management decision to permit operation of information systems in specific environments at an acceptable level of risk, based on the implementation of an approved set of technical, managerial, and procedural safeguards.

(U//~~FOUO~~) When accrediting systems, TSS uses the National Institute of Standards and Technology (NIST) Risk Management Framework to determine the appropriate level of risk mitigation to protect systems, information, and infrastructure. NIST Special Publication 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*, February 2010, describes the six steps in the framework.

~~TOP SECRET//SI//NOFORN~~

TOP SECRET//SI//NOFORN

ST-14-0002

- (U//~~FOUO~~) Categorize the information system and the information processed, stored, and transmitted by the system based on an impact analysis (risk assessment),
- (U//~~FOUO~~) Select an initial set of basic security controls for the information system based on the security categorization and supplementing the security controls as needed based on an organizational assessment of risk and local conditions,
- (U//~~FOUO~~) Implement the security controls and describe how the controls are employed within the information system and its environment of operation (system developer),
- (U//~~FOUO~~) Assess the security controls using appropriate assessment procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system (independent testing by TS),
- (U//~~FOUO~~) Authorize information system operation based on determination of the risk to organizational operations and assets, individual or other organizations, and the nation resulting from the operation of the information system and the decision that this risk is acceptable, and
- (U//~~FOUO~~) Monitor the security controls in the information system on an ongoing basis including assessing control effectiveness, documenting changes to the system or its environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to designated organizational officials.

(U//~~FOUO~~) Before a system is authorized to be put on a network, it must go through the accreditation process and be approved by TS. Once implemented, systems are (b)(3)-P.L. 86-36 subject to reaccreditation every three years or whenever significant changes occur that may affect the risk assessment. The dates through which the E&AA §702 repositories are accredited are listed in Table 300.

(U//~~FOUO~~) Table 30. Accreditation Status of NSA [REDACTED]

| (TS//REL TO USA, FVEY)   | System named in the System Security Plan (SSP) | (TS//REL TO USA, FVEY) |
|--------------------------|--|------------------------|
| (b)(1) (b)(3)-P.L. 86-36 |  |                        |

TOP SECRET//SI//NOFORN

TOP SECRET//SI//NOFORN

ST-14-0002

(U//~~FOUO~~) **Certification** In addition to system accreditation, all systems containing FISA data must be certified by TV4, the NSA authority for certifying automated systems to ensure they are compliant with the legal and policy regulations protecting USP privacy. DoI and the HSC are notified when NSA designates a new [REDACTED]

(U//~~FOUO~~) In 2010, NSA began certifying HSSAs systems as part of an effort to ensure that they comply with the legal and policy regulations protecting USP privacy. This included the repositories that contain FAA §702 metadata. Personnel from various organizations within SID and TID performed the initial certifications. TV subsequently assumed responsibility for system certification and developed the NSA corporate database for registering NSA systems, their compliance certification and data flows. It is NSA's authoritative source for all compliance certifications.

(b)(3)-P.L.86-36

(U//~~FOUO~~) The Agency's certification process currently evaluates system controls for compliance with programmatic requirements and age-off, data access, querying, dissemination, data tagging, targeting, and analytical processes. The six mission functional areas are delineated by the Comprehensive Mission Compliance Program (ODOC administers). Through this program, compliance certification requirements are developed to address required compliance controls. The compliance requirements, administered by the TV4 requirement team, form the basis for the criteria against which systems are certified for compliance.

(U//~~FOUO~~) To be certified to handle FISA data, systems must receive TV certification through the Compliance Certification process. The TV4 certification dates for the [REDACTED] that contain FAAA§ §702 data and which can be used as sources to support dissemination are listed in Tables B.1.

(U//~~FOUO~~) **Table 31. Compliance Certification Status of NSA**

(b)(3)-P.L.86-36

(TS//REL TO USA, FVEY)

| System     | [REDACTED] | Certification Date |
|------------|------------|--------------------|
| [REDACTED] | [REDACTED] | [REDACTED]         |

(b)(1)

(b)(3)-P.L.86-36

(U//~~FOUO~~) TV provided new compliance certification guidance in May 2014. Systems other than those being decommissioned in this transition, which meet the following criteria should be certified by TV:

(b)(3)-P.L.86-36

- (U//~~FOUO~~) Systems with two significant system-related incidents in a twelve month period or three total,
- (U//~~FOUO~~) FISA systems that have not been certified within two years,

TOP SECRET//SI//NOFORN

TOP SECRET//SI//NOFORN

ST-14-0002

- (U//~~FOUO~~) Systems with a major upgrade affecting compliance or functionality, or
- (U//~~FOUO~~) Systems planning go process under a new authority (e.g. addition of FISA data).

(U//~~FOUO~~) Owners of all affected FISA systems were notified in June 2014 that they should complete recertification, if their systems met these guidelines, within six months. [ ] of the repositories [ ] [ ] are scheduled to be decommissioned and were exempted from this requirement.

(b)(3)-P.L. 86-36

#### (U) Data flow management

(C//REL TO USA, FVEY) USSIDs define a set of controls and operating procedures for the United States SIGINT System. USSID IDA3511, *Data Acquisition Directorate Targeting and Data Flow Management*, defines a process intended to assure that only desired SIGINT is delivered to intended users in the time frame and format required.

(S//SI//REL TO USA, FVEY) [ ] is responsible for governing end-to-end management of Internet and telephony data collection. [ ] houses the access data managers responsible for testing and setting up new data flow paths that traverse the SIS processing infrastructure. The [ ] Data Governance Team governs the processing and distribution of data collected within NSA's SIGINT system, oversees the documentation and review of all new dataflow requests, and implements processes designed to ensure that NSA compliance standards are maintained throughout the development of new data flows.

(b)(3)-P.L. 86-36

(S//SI//REL TO USA, FVEY) The Data Governance Team manages the data flow process. Customers must complete Dataflow Management Requests (DMRs) to initiate or modify dataflows. DMRs require detailed information, including the status of system certifications, system accreditation, the type of data to be processed [ ] authorities for collection, and documentation of data flows. DMRs are evaluated and approved by a triage team [ ] Upon triage team concurrence, the DMR is given to the [ ] Targeting and Tasking and [ ] Data Delivery organizations for testing and implementation. DMRs are complete once all required approvals are obtained and data flows become operational.

(b)(3)-P.L. 86-36

#### (U) Data tagging

(U//~~FOUO~~) Historically, NSA has managed data access by implementing restrictions on data storage, including the use of logical database partitions. Data flows were designed to place data in these partitions; for example, according to the FAA §702 certification under which the communications were acquired to access the data, personnel had to have appropriate training and be given access to certain systems and missions matching the data partitions where the data was stored.

TOP SECRET//SI//NOFORN

~~TOP SECRET//SI//NOFORN~~

ST-14-0002

(U//~~FOUO~~) As NSA [redacted] new mechanisms for [redacted] (b)(3)-P.L. 86-36 storing and accessing data are being developed. Data tags are created for each collection record identifying the authority under which the data was collected, as well as several other pieces of information used in managing the data over its life.

[redacted]

[redacted] Thus, to access raw data acquired under the [redacted] (b)(3)-P.L. 86-36 certification for FAA §702, analysts must be approved for access to such collection as part of an authorized mission and fulfill the training requirements for the authority.

(U//~~FOUO~~) Data tags also serve to maintain compliance with limitations on the scope of queries, as well as age-off and purge requirements.

(U//~~FOUO~~) Table 32 summarizes the repository provisions of the FAA §702 targeting and minimization procedures and the controls NSA implemented to maintain compliance.

#### **(U) Table 32. FAA §702 Repository Provision and Controls**

(U//~~FOUO~~)

| Provision   | Control  |
|---|--|
| (U// <del>FOUO</del> ) NSA has established processes for ensuring that raw traffic is labeled and stored only in authorized repositories. | (U) All systems processing FAA §702 data must complete a security accreditation process.<br>(U) All FAA §702 repositories are certified compliant with the legal and policy regulation protecting USP privacy.<br>(U// <del>FOUO</del> ) Data flows must be approved by [redacted] and SV to ensure compliance.<br>(U// <del>FOUO</del> ) Data tags are applied to identify the authority under which the information was acquired. The tags also serve to manage access to and retention of the data. |

(U//~~FOUO~~)

(b)(3)-P.L. 86-36

#### **(U) Access and Training**

##### **(U) Provisions of FAA §702 certifications**

(U) The FAA §702 targeting procedures state that NSA will develop and deliver training to ensure that intelligence personnel responsible for approving the targeting of persons under that authority as well as analysts with access to the raw data acquired pursuant to FAA §702, understand their responsibilities and the procedures that apply to this acquisition.

71 (C/REL TO USA, FVEY)

|    |    |    |   |   |
|----|----|----|---|---|
| CS | To | NN | N | ~ |
|----|----|----|---|---|

~~TOP SECRET//SI//NOFORN~~

TOP SECRET//SI//NOFORN

ST-14-0002

## (U) Control framework for restricting access to FAA §702 collection to authorized personnel

(TS//SI//NF) NSA requires that users having access to FAA §702 data have one or more credentials, be current on required training and be assigned to approved missions.

(b)(1)  
(b)(3)-P.L. 86-36

(S//SI//NF) Required credential One [redacted] credential is needed to access FAA

§702 data:

is required to access data collected under the

[redacted] FAA §702 certifications. [redacted]

(C//REL TO USA, FVEY) Obtaining the credential To obtain any of the [redacted] credentials, a request must be submitted in [redacted]. Only individuals who hold the requested credential may submit a request for the credential. The request is first reviewed by the Associate Directorate for Security and Counterintelligence (Q) to determine whether the applicant has satisfied certain security criteria. If approved by Q, the request is forwarded to SV for final adjudication. SV reviews the request, verifying that the individual is current on required training and that the request includes a valid mission classification. If all requirements are met, SV approves the credential in [redacted] for entry to NSA's security database. [redacted] retrieves information from [redacted] and several other corporate authoritative source systems that provide the status of individuals' approved missions, training, and clearances. Using this information, [redacted] calculates daily a list of individuals who qualify for FAA §702 access. NSA systems use the information from [redacted] to determine what data the individuals are authorized to access. SID maintains the authority rules, which determine what [redacted] verifies for individuals to access data.

(U//FOUO) Obtaining access to mission resources SID policy designates [redacted] as NSA's tool for the proper administration and implementation of access to SIGINT data in NSA repositories; it facilitates the administrative process of acquiring access to tools and databases. Access sponsors submit individuals for access. The sponsors determine the appropriate SIGINT authority for users, assigning them to a mission documented in the mission correlation table, a master list of all analytic production elements that have been approved for SIGINT missions. The table facilitates database access by providing a record of databases needed to perform SIGINT missions. The access sponsor nominates a user for access to raw SIGINT databases, sources, and tools in support of a stipulated mission. The sponsor ensures that auditors are assigned to the mission to review queries of mission audit data. [redacted] feeds user access information to [redacted]

(b)(3)-P.L. 86-36

<sup>72</sup> (U//FOUO) The [redacted] credential was originally established for FISA data and requires training in NSA's Standard Minimization Procedures for FISA information. Later, different versions of [redacted] [redacted] were established for particular categories of FISA. [redacted] permits access to FAA §702 data acquired before the establishment of the [redacted] credential in [redacted]

TOP SECRET//SI//NOFORN

TOP SECRET//SI//NOFORN

ST-14-0002

(U//~~FOUO~~) Maintaining accesss Automated and manualpprocedures provide assurance of continuing eligibility to access FAA §702 data. Users and access sponsors are responsible for removing user's accesss whether they no longer qualify for a mission. Each [ ] mission is also required to have an intelligence oversight officer who performs periodic reviews to ensure that individuals assigned to missions are still eligible foraccesss.

(U//~~FOUO~~) Enforcement of required training is supported by the production of automated notices to individuals well in advance of their training expirationdate. Notices areproduced at regular intervals until the training is completed. If training expires, the individual is automatically removed from access to FAA §702 data.<sup>73</sup>

~~(C//REL TO USA, DIVEND)~~ [ ] calculates daily a list of individuals who qualify for FAA §702 access. [ ] interfaces with several corporate authoritative source systems that provide the status of individual's approvedmissions, training, and clearances. For systems that ussdatalaggs, user information in [ ] is compared with the data tag supplied to the communications before giving the individuals access to the data. If the user doesnot possess the combination of requirements identified in the data tag, access to that data isdenied.

(U//~~FOUO~~) Appropriate and adequate training NSA/CSS Policy 1-23 requires that Agency personnel complete IO training annually..

(U//~~FOUO~~) To qualify for accesss to data acquired under anFAA §702 certification, persons must have completed specific training courses within the last 12 months. All courses are developed by NSA's ADET in conjunction with the CIO/GC mission subject matter experts and mission operational professionals. All NSA analysts who perform targeting functions must take the first three courses listed above the last is mandatory only for personnel requiring access to FAA §702 data.

- (U//~~FOUO~~) OVSC1000 - NSA/CSS Intelligence Oversight Training -the Agency'scored course provided to the workforce to maintain ahigh degree of sensitivity to and understanding of intelligence laws, regulations, and policies associated with the protection of U.S. person privacy rights. Personnel are familiarized with themajorelements of the four core IO documents: Executive Order 12333, as amended, Department of Defense Regulation 5240.1-R, Directive Type Memorandum 0805052 and NSA/CSS Policy 1-23. OVSC1000 is web-based and includes knowledge checks for proficiency.<sup>74</sup>
- (U//~~FOUO~~) OVSC1100 - Overview of Signals Intelligence Authorities -the SIGINT corel course provides an introduction to various legal authorities

<sup>73</sup> (U//~~FOUO~~) [ ] does not verify the individual's FAA §702 training status. [ ]

<sup>74</sup> (U//~~FOUO~~) E.O. 12333, *United States Intelligence Activities*; DoD Regulation 5240.1-R, *Procedures Governing the Activities of DoD Intelligence Components That Affect US Persons*; DTM-08-052, *DoD Guidance for Reporting Questionable Intelligence Activities and Significant or Highly Sensitive Matters*.

TOP SECRET//SI//NOFORN

governing NSA operations. Upon completion, personnel should be able to identify applicable surveillance authorities at a high level, define the basic provisions of the authorities, and identify situations requiring additional authority. OVSC1100 is web-based and includes knowledge checks for proficiency. All personnel in the U.S. SIGINT System (USSS) working under NSA SIGINT authority with access to raw SIGINT are required to complete OVSC1100.

- (U//~~FOUO~~) OVSC1800 - *Legal Compliance and Minimization Procedures* -- an advanced SIGINT intelligence oversight course which explains policies, procedures, and responsibilities within missions and the obligations of the USSS to protect US person and foreign partner privacy rights. OVSC1800 is web-based and includes competency exams [redacted]

[redacted] Personnel who do not pass the test after [redacted] attempts must complete remedial training. All analysts in the USSS working under DIRNSA SIGINT authority with access to raw SIGINT are required to complete OVSC1800 annually. (b)(3)-P.L. 86-36

- (U//~~FOUO~~) OVSC1203 FISAA Amendments Act (FAA) "Section 702, explains the legal policies and targeting and minimization procedures FAA mandates. The course is web-based and includes a competency exam [redacted]

[redacted] Personnel who do not pass the test after [redacted] attempts must complete remedial training. All analysts who require access to FAA §702 data must take this course annually.

(U//~~FOUO~~) Other courses are also required before analysts can access NSA targeting tools. The first four of these are required for all NSA analysts who perform targeting functions, while the last is mandatory only for those analysts targeting under FAA §702.

- (U//~~FOUO~~) CRSK1300, Foundations of Smart Targeting, a web-based course that covers targeting policy processes and concepts, available assistance, targeting tools, research, and collection.
- (U//~~FOUO~~) CRSK1301, Foundations of Smart Targeting: Research, available in web-based format beginning January 2015, the course focuses on elements of the targeting process requiring research, the research process, and the tools and databases used in research.
- (U//~~FOUO~~) CRSK1302, Foundations of Smart Targeting: Targeting, a web-based course that includes collection sources, considerations, the target workflow process, creating TRs, finding and assessing collection results, and documenting sources.
- (U//~~FOUO~~) CRSK1303, Foundations of Smart Targeting: Targeting Maintenance, a web-based course that focuses on resolving compliance problems, managing traffic, and maximizing the intelligence value of tasked selectors.

~~-TOP SECRET//SI//NOFORN-~~

ST-14-0002

- (U//~~FOUO~~) CRSKIB094, FAA Section 702 Practical Applications, a web-based course required for all NSA analysts who conduct targeting under FAA §702. It is scenario-based and addresses compliant TIRs, targeting maintenance, and incident reporting.

(U//~~FOUO~~) **Adjudicator training** In addition to the above courses, mission personnel who grant final approval of FAA §702 TRs must take a course on the approval process, be approved by their FAA §702 Mission lead, receive hands-on training by personnel with adjudication experience, and be approved by S2 Mission and Compliance staff. Upon approval, elements in SID will upgrade the individual's access role in [redacted] to allow adjudication of TRs. (b)(3)-P.L. 86-36

- (U//~~FOUO~~) CRSKJ 305 - FAA Section 702 Targeting Adjudication – a course that explains NSA resources for validating selectors and foreignness explanations in [redacted] TRs, determining whether submitted TRs should be approved, and follow-up actions after a TR has been approved or denied.

#### (U) **Access requirements for technical personnel to FAA §702 repositories**

(U//~~FOUO~~) Technology Directorate personnel who directly support repositories and systems that contain raw SIGINT data or activities that utilize raw SIGINT must complete OVSCI1000, OVSCI100, and OVSCI1806 training annually. OVSC 1806 is the same course as OVSC1800 (see above) but has an additional lesson on the system compliance certification process. Technical personnel who support FISA systems and whose responsibilities may include direct access to FISA data are also required to attend a briefing administered by OGC and TV. Upon completion of the briefing, SW updates [redacted] recording the user's attendance at the briefing and their authorization for access.

#### (U) **Identification of access vulnerability in [redacted]**

(U//~~FOUO~~) [redacted] is one of the [redacted] scheduled to be decommissioned in 2017. [redacted] relies on a combination of [redacted]

[redacted] to protect access to data. [redacted] does interface with [redacted] however, it does not verify that an individual is current on training as part of its access control.<sup>76</sup>

(C//~~REL TO USA, FVEY~~) [redacted] an individual with authorized access to FISA data discovered that FAA §702 data had been included in the results of a query of [redacted] data. The individual that received FAA §702 training when he was

(U//~~FOUO~~) [redacted]

<sup>76</sup> (U//~~FOUO~~) [redacted] is NSA's Corporate Authorization Service. See the Obtaining the Credential section for more information and [redacted]. (~)-P.L. (b)(3)-P.L. 86-36

~~-TOP SECRET//SI//NOFORN-~~

assigned to a different mission so her access to the data was not in violation of the FAA §702 targeting and minimization procedures. However, the access did violate SID policy because the mission to which the individual was assigned was not authorized for FAA §702.<sup>77</sup> Investigation of the occurrence led to the discovery that personnel without the required FAA §702 training could access FAA §702 data in [ ] if they have the [ ] credential.<sup>78</sup> To date, no incidents have been identified of individuals who have not received FAA §702 training querying [ ] and receiving FAA §702 data.<sup>79</sup>

(U//FOUO) When SV personnel discovered this vulnerability they worked with TD to initiate corrective measures. [ ] was updated to add new COIs to FAA §702 data collection or after that date. The new COIs emulate the access controls required for other FAA §702 systems, including controlling access based upon the authority under which it was obtained. [ ] A similar process will be implemented to address access controls for data obtained [ ]. A review is currently underway regarding actions to take for data [ ].

(U//FOUO) Table 33 summarizes the access and training provisions of the FAA §702 targeting procedures and the controls implemented by NSA to maintain compliance.

(b)(3)-P.L. 86636

(U) Table 33. Access and Training Provisions and Controls

(U//FOUO)

| Provision   | Control   |
|---|---|
| (U) NSA will develop and deliver training regarding the applicable procedures to ensure that intelligence personnel responsible for approving the targeting of persons under FAA §702, as well as analysts with access to the acquired foreign intelligence information, understand their responsibilities and the procedures that apply to this acquisition. | (U//FOUO) NSA has a list of courses required annually for analysts to qualify for access to data acquired under FAA §702. This includes OVSC1203, a course specific to FAA §702.<br>(U//FOUO) To access NSA targeting tools, all analysts must complete four courses on targeting. Analysts targeting under FAA §702 must also take a course on application of the authority.<br>(U//FOUO) Adjudicators (who grant the final approval of TTRs under FAA §702) must also complete a course on adjudication specific to the authority.<br>(U//FOUO) Technology Directorate personnel who support FISA systems must complete OVSC1000, 1100 and 18006 annually and attend a briefing administered by OGC and TV. |

<sup>77</sup> (CROSS TO USA, FVB) SID Management Directive 421 states that FISA access is based on current mission need and does not follow individual analysts when they move to new missions or locations unless specified in the document authorizing the assignment. Persons changing missions, jobs, or locations must provide re-justification to SV through their management chains for FISA access or access to unminimized, unevaluated content in the new positions.

<sup>78</sup> (U//FOUO) Without a [ ] credential, analysts cannot access FAA §702 data and most other types of FISA data. The [ ] credential was originally established for FISA data and requires training in NSA's standard minimization procedures for FISA information.

<sup>79</sup> (TS//SI//NOFORN) Of NSA's [ ] SIGINT missions authorized for FISA access, [ ] are also authorized to access FAA §702 data.

(b)(1)  
(b)(3)-P.L. 86636

~~-TOP SECRET//SI//NOFORN~~

ST-14-00002

|   |  |
|---|--|
| (U) NSA has established processes to ensure that raw traffic is accessible in authorized repositories only to those who have had the proper training. | (U//FOUO) Access to FAA §702 foreign intelligence and the ability to submit and approve targeting under the authority require certain credentials and access to mission resources (databases, sources and tools). The approval is not granted unless the required training has been completed. (See above information regarding access.) |
|---|--|

(b) (3)-P.L. 86-36

(U//FOUO)

**(U) Querying Repositories of Collected FAA §702 Data****(U) Provisions of FAA §702 certifications-queries**

(U) Minimization procedures permit use of computer selection terms to scan storage media containing communications acquired pursuant to FAA §702 and to select communications for analysis with certain limitations. Query selection terms (e.g., telephone numbers and key words and phrases) must be formulated in a manner reasonably likely to return foreign intelligence information. Collection obtained through NSA upstream Internet collection techniques may not be required using selection terms of an identifiable USP.

**(U) Compliance controls-query compliance**

(U//FOUO) Queries of raw SIGINT databases are subject to USSID CR1610, *SIGINT Production and Raw SIGINT Access*, revised 12 February 2013, which requires that:

- (U//FOUO) All user organizations designate two auditors to review daily those queries presented for their review.<sup>80</sup>
- (U//FOUO) Auditors be familiar with the targets and types of queries executed within their missions.
- (U//FOUO) SV provide training for new auditors on their responsibilities and certify them as compliant before conducting audits.<sup>81</sup>
- (U//FOUO) SV conducts periodic spot audits of interactive raw SIGINT database queries, verifying that selectors were foreign on the data the paper audit is performed and examining the query terms to determine compliance with NSA policy.<sup>82</sup>
- (U//FOUO) NSA maintain a non-editable file of all such database queries for a minimum of one year.

<sup>80</sup> (U//FOUO) [ ] NSA implemented an approach to query review that uses stratified sampling based upon historical rates of queries identified as "reportable" to determine the queries from each database to be presented for auditor review. The [ ] system passively logs queries, but the queries are not subject to audit. NSA is developing a process to provide additional oversight for queries against this system.

<sup>81</sup> (U//FOUO) Auditors are now required to take *NSA Raw Traffic Database Auditor Training* (OVSC3101) every two years and must be cleared to the security level required for the authority under which the analyst performed the query subject to audit.

<sup>82</sup> (U//FOUO) The system used to test foreignness [ ] does not maintain an historical record of foreignness of the tested selector.

~~-TOP SECRET//SI//NOFORN~~

~~-TOP SECRET//SI//NOFORN~~

ST-14-0002

- (U//~~FOUO~~) All queries be directed by a foreign intelligence purpose and
- (U//~~FOUO~~) An audit record of the selection terms be created and reviewed per NSA policy by the originating organization.

(b)(3)-P.L. 86-36

(U//~~FOUO~~) Mission auditors are assigned to each mission using the [ ] tool described in the access section. The tool requires that missions have designated auditors before new personnel can be approved for the missions. Auditor qualifications include target knowledge, expertise in the mission area, familiarity with the type of queries to be reviewed, ability to mentor analysts to improve query execution, attainment of all credentials required for the data reviewed and completion of all required training. Queries presented to auditors are required to be audited within 24 hours of receipt or on the next normal day.

(U//~~FOUO~~) SV developed OVSC3101, *NSA Raw Traffic IDatabase Audit/Training*, to prepare auditors for post query review. The course provides instruction on use of the corporate query audit system, incident identification, incident reporting and maintenance of records of audits (to support SV super audits and DoJ/ODNI reviews).

(S//SI//REL TO USA, FY1X) The [ ] system, a legacy system which predates USSID CRT610 and is scheduled to be decommissioned, does maintain a log of queries for five years. The system has not yet been modified to provide these

(b)(3)-P.L. 86-36 query logs to the corporate logging and auditing system.

(U//~~FOUO~~) Queries not using USP selection terms [ ]

(U//~~FOUO~~) IfAA §702 systems provide records of queries to the corporate logging and auditing system for user generated queries of raw SIGINT content.<sup>83</sup> These records are then used to facilitate query reviews by auditors and SV query oversight. These systems also maintain records of query reviews.

(U//~~FOUO~~) Auditors examine queries to determine whether they have a valid foreign intelligence purpose. Auditors also evaluate query selection terms to determine whether they were constructed so as to avoid obtaining information on USPs. The review is intended to balance the pursuit of foreign intelligence and protection of USPs' Fourth Amendment rights. When a tasked FAA §702 selector is used as a query term and the selector is foreign to the system, the query is rejected and the system does not present the query for review by an auditor because the term has been reviewed by a releaser and an adjudicator as part of the TIR approval for tasking during the targeting process.<sup>84</sup> If a tasked selector is used as a query term and the

<sup>83</sup> (U//~~FOUO~~) One of the [ ] does not send query records to the NSA Corporate Logging and auditing system. This system is scheduled to be decommissioned. (b)(3)-P.L. 86-36

<sup>84</sup> (U//~~FOUO~~) The query auditing and logging system obtains current tasked selectors from [ ] and verifies their foreignness against NSA SIGINT databases.

~~-TOP SECRET//SI//NOFORN-~~

TOP SECRET//SI//NOFORN

ST-14-0002

selector is not foreign, it is subject to review by an auditor. Queries using selection terms that are not approved selectors are subject to auditor review.

#### (U//FOUO) Provisions of FAA §702—queries using USP selection terms

(U//FOUO) A 3 October 2011 FISC Order approved the use of modified minimization procedures that permit queries of data collected under the authority only for foreign intelligence purposes, using USP query terms subject to specific NSA review procedures and external oversight. Such queries can only be performed using FAA §702 telephony communications and Internet communications obtained from downstream collection. Use of USP identifiers to query FAA §702 collection must be approved in accordance with NSA procedures. NSA is required to maintain records of all USP identifiers approved for use as selection terms. These query procedures are subject to oversight by DoJ and ODNI.

#### (U//FOUO) Compliance controls—queries with USP selection terms

(U//FOUO) NSA adopted internal procedures governing use of USP identifiers for queries of communications collected under FAA §702. Upstream Internet collection is not approved for such queries. DoJ and ODNI reviewed and approved these procedures. The Senate and House Intelligence Committees were informed of these changes. There are three sets of procedures for approval of these queries:

- (U//FOUO) Queries of metadata,
- (U//FOUO) Emergency queries of content, and
- (U//FOUO) Non-emergency queries of content.

(U//FOUO) NSA's annually required course on FAA §702, OWSCI2003, includes training on the use of USP identifiers to query raw data collected under the authority. The NSA FAA web page also contains the documented and approved procedures for these queries. Although metadata queries are not subject to pre-approval, the query and a foreign intelligence justification must be recorded to support external oversight. The justification must document the analytic knowledge linking the selector to a foreign target or foreign intelligence purpose. Content queries using USP identifiers are subject to pre-approval by SS2, SV, and OGC. SV maintains records of all queries using USP identifiers and includes such queries in its query oversight.

(U) Table 34 summarizes the query provisions of NSA's FAA §702 minimization procedures and the controls implemented by NSA to maintain compliance.

TOP SECRET//SI//NOFORN

## (U) Table 34. Query Provisions and Controls

(S//SI//REL TO USA, FVEY)

| Provision  | Control   |
|--|---|
| <p>(U) Storage media (data repositories) containing communications acquired pursuant to FAA §702 may be queried to identify and select communications for analysis. Query terms, such as telephone numbers and key words or phrases, will be limited to those selection terms reasonably likely to return foreign intelligence information.</p> <p style="text-align: center;">(b)(3)-P.L. 86-36</p> | <p>(U) Queries of FAA §702 databases may only be conducted for foreign intelligence purposes and are subject to review by mission auditors who must have target knowledge expertise in the mission area and have completed training on raw traffic database auditing. The review evaluates whether the query was for a valid foreign intelligence purpose.</p> <p>(U//FOUO) SV conducts periodic super audits of these queries.</p> <p>(S//SI//REL TO USA, FVEY) NSA maintains a file of all database queries for at least one year in the corporate logging and auditing system for user generated queries on raw SIGINT content. [REDACTED]</p>   |
| <p>(U) Identifiers of an identifiable USP may not be used as terms to query any Internet communication acquired through upstream Internet collection. Use of USP identifiers as terms to query communications must be approved in accordance with NSA procedures. NSA will maintain records of all USP identifiers approved for use as selection terms.</p>  | <p>(U//FOUO) All personnel receive annual training on USP query procedures which can only be performed for foreign intelligence purposes against FAA §702 telephony communications and Internet communications. [REDACTED] The SV web page provides instructions for requesting approval of such queries, using a process that DoJ and ODNI approved.</p> <p>(U//FOUO) Queries of upstream Internet collection using USP terms are prohibited.</p> <p>(U//FOUO) Queries of metadata are not subject to pre-approval, but the query and foreign intelligence justification must be documented.</p> <p>(U//FOUO) Content queries using USP terms follow request and documentation procedures and are subject to pre-approval by SV and OGC.</p> <p>(U//FOUO) SV maintains records of all queries using USP identifiers and includes these queries in its oversight of query review.</p> |
| <p>(U//FOUO) DoJ and ODNI will conduct oversight of NSA's queries using USP identifiers.</p>   | <p>(U) See the Oversight section.</p>   |

(S//SI//REL TO USA, FVEY)

## (U) Sharing and Dissemination

## (U) Sharing

(U//FOUO) As stated in the Access and Training section, targeting procedures require that all personnel accessing or otherwise handling raw data acquired pursuant to FAA §702 must be current on training for the authority. This imposes restrictions even within NSA on the use of information obtained under this authority.

(U) Unminimized communications acquired pursuant to FAA §§702 may be provided to the CIA and FBI for target search has been classified to NSA. Each agency has minimization procedures for handling data collected under this authority and must

~~-TOP SECRET//SI//NOFORN-~~

ST-14-0002

handle communications provided by NSA in accordance with these procedures. Currently, unminimized data shared with the CIA and FBI is limited to communications derived from downstream collection.

**(U) Dissemination**

(U) The NSA minimization procedures apply to dissemination of all information acquired under FAA § 702, including non-publicly available information concerning USPs acquired by targeting non-USPs approved under the NSA targeting procedures. There are several restrictions on dissemination of information acquired under this authority.

- (U//FOUO) **Discrete Communications within an MCT** Analysts seeking to disseminate information obtained from discrete communication within an MCT must assess whether the communication is eligible for dissemination (e.g., non-domestic communication) and document that assessment in the comments field of the reporting tool in a manner that supports internal and external oversight.
- (U//FOUO) **Attorney-Client Communications** Dissemination of USP attorney-client privileged communications must be reviewed by the NSA OGC. NSA must cease review of communications between person known to be under criminal indictment in the United States and an attorney representing that individual in that matter, segregate such communications, maintain a record of the identified attorney-client communications, and notify DOJ so that appropriate procedures may be established to protect such communications from review or use in a criminal prosecution, while preserving foreign intelligence information in the communication.
- (U//FOUO) **Domestic Communications** A domestic communication may only be disseminated if DIRNSA has approved a destruction waiver for that communication, documenting its eligibility for retention and dissemination. Such communications must contain information that meets one of four criteria: significant foreign intelligence, criminal database information necessary to assess a communication's vulnerability, evidence of a crime, or information concerning a threat of serious harm to life or property. Communications acquired where there was reasonable belief at the time of tasking that target was a non-USP located outside the United States and not eligible for destruction waivers. If a waiver has been issued, NSA may share domestic communications that do not have foreign intelligence value but are believed to contain evidence of a crime with appropriate federal law enforcement authorities in accordance with applicable laws and regulations.<sup>85</sup> Without a destruction waiver, NSA is authorized to notify the FBI if information in a domestic communication indicates that target has entered the United States. The Agency may also provide information to the CIA and

<sup>85</sup> (U) 50 U.S.C. §§ 1806(b) and 1825(c) require that the communications be released with a statement that the Attorney General must approve use of the information in a criminal proceeding. USC § 1806(b) is not limited to FAA § 702 domestic communications; it applies to all disseminations to law enforcement.

~~-TOP SECRET//SI//NOFORN-~~

FBI for collection avoidance purposes. NSA may retain domestic communications shared with the CIA and FBI for six months and may use strict further use or dissemination of communications whose destruction has been waived by placing the identifiers for these communications on the MPL.

- (U) **Foreign Communications of or Concerning USPs** These communications may be disseminated, if the identity of the USP is deleted and a generic term substituted so that the information cannot reasonably be connected with an identifiable USP. This process is referred to as "masking." Otherwise, dissemination of intelligence based on such communications may only be made to recipients requiring the identity of the USP to perform their official duties and only if at least one of eight additional requirements is met:
  - (U) The USP consented to dissemination or the information is publicly available,
  - (U) The USP identity is necessary to understand the foreign intelligence information or assess its importance,
  - (U) The communication or information indicates that the USP may be a foreign power, an agent of a foreign power, residing outside the United States and holding an official position in the government or military forces of a foreign power, a corporation or other entity owned or controlled directly or indirectly by a foreign power, or acting in collaboration with an intelligence or security service of a foreign power and the USP has or has had access to classified national security information or material,
  - (U) The USP may be the target of intelligence activities of a foreign power,
  - (U) The USP is engaged in unauthorized disclosure of classified national security information (only if the originating agency has verified that the information has been properly classified),
  - (U) The USP communication was authorized by a court demand the communication may relate to the foreign intelligence purpose of the surveillance,
  - (U) The USP may be engaging in international terrorist activities, or
  - (U) There is evidence that the USP is engaging in a criminal activity.
- (U) **Foreign Communication of or Concerning a Non-USP** may be disseminated in accordance with other laws, regulations and policies, provided that the communications are eligible for retention under FAA § 702.
- (U) **Collaboration with Foreign Governments** Consistent with the authority accorded NSA by E.O. 12333, the Agency maintains cryptologic liaison relationships with certain foreign governments. Information derived from FAA § 702 collection that has been evaluated for foreign intelligence and minimized for USP information may be disseminated to these foreign

~~TOP SECRET//SI//NOFORN~~

ST-14-0002

governments.<sup>86</sup> Dissemination of information of or concerning a USP must comply with the restrictions described in Foreign Communications or Concerning USPs above, as well as with those described for MCTs above. NSA is permitted to disseminate unminimized communications to foreign partners to obtain technical or linguistic assistance to determine the meaning or significance of the information.<sup>87</sup>

**(U) Sharing FAA §702 with authorized NSA personnel**

(U//FOUO) Analysts authorized to access FAA §702 communications are trained to ensure that individuals with whom they wish to discuss such communications have appropriate credentials. [REDACTED] permits review of an individual's training and clearances. The training also addresses NSA policy which states that e-mailing unminimized and unpublished data to anyone, even other NSA personnel, violates compliance controls such as effective auditing.

(b)(3)-P.L. 86-36

**(U) Provision of unminimized communications to CIA and FBI**

(U//FOUO) As described in the Targeting section, NSA must approve selectors nominated by these agencies based upon compliance with NSA targeting procedures.

For approved selectors, Internet communications [REDACTED] [REDACTED] are routed to the requesting agency [REDACTED] based upon information in the TR. NSA policy states that analysts should not share unminimized and unevaluated communications received pursuant to this collection with the CIA and FBI for selectors tasked to both of those agencies. Collaboration on such collection is permitted when analysts from the CIA or FBI access the unminimized communications from their own agencies' FAA §702 data repositories. The required annual FAA §702 course, OVSCJ203, provides training on these restrictions which are designed to assure accountability of dissemination if recall or purge becomes necessary.

(b)(3)-P.L. 86-36

**(U) General dissemination requirements**

(U//FOUO) **Limits on use of reported FAA §702 communications** Analyst training (OVSCJ203) instructs that "use or disclosure of information derived from FAA §702 communications in any criminal proceeding, immigration proceeding or any other legal or administrative proceeding is prohibited without the advance authorization of the Attorney General of the United States." To prevent such use, NSA internal procedures require that dissemination of FAA §702 derived information include the "Intelligence Purposes Only" caveat that prohibits the use of the information without approval. This is included in the FAA §702 training.

<sup>86</sup> (U//FOUO) Collected traffic that has been evaluated to determine whether it contains foreign intelligence and has been subject to minimization to protect USP identities is referred to as evaluated/unminimized traffic or EMT.

<sup>87</sup> (U) Dissemination for technical or linguistic assistance is subject to specific restrictions limiting the use of the information by the foreign government to translation or analysis of the communications, allowing dissemination only to the individuals performing the analysis or translation, restricting the foreign government from making a permanent record of the information, and requiring destruction or return to NSA of the information disseminated.

~~TOP SECRET//SI//NOFORN~~

(U//~~FOUO~~) **Reporting documentation** Consistent with the purge requirements in the minimization procedures, NSA is required to account for and must be able to trace its disseminations based on FAA §702 communications. The annual training addresses the documentation that analysts must complete to fulfill this requirement:

- (S//NF) The collection authority (specific FAA §702 certification) [redacted]  
[redacted] piece of traffic used in the report, and (b)(3)-P.L.86636
- (U) A source verification statement documenting a decision for each piece of traffic and confirming that the source was not ineligible for retention or subject to purge. A new reporting tool, first introduced in 2013, performs the source verification automatically. Successful completion of this process with no flags confirms that the traffic may be used as a source for reporting.

~~(S//SI//REL TO USA, FVEY)~~ An NSA reporting policy document, *Sourcing Requirement and Verification Guidance*, ISS-054-10, revised 8 May 2012, provides reporting and dissemination guidance. The policy requires that individuals releasing reports verify that the reports do not contain information that should have been purged from raw SIGINT databases. This must be performed within 24 hours of the report release using the Master Purge List. SIGINT reporters are also required to include traffic source identifiers for all reports and enter source verification statements in the reporting tool to confirm that this review has been performed.

~~(S//SI//REL TO USA, FVEY)~~ The primary analyst reporting tools used in 2013 performed automated verification of sources against NSA's [redacted] at the time of report release. If none of the source records for the report matched records in the purge system, the report would be released. If a match to the identifier for a purged record was found, the release would be stopped and the individual releasing the report would be notified. The policy requires that a manual source verification check be performed for reports released through means other than automated source verification. In 2014, a new analyst reporting tool was implemented that also includes automated source verification (see the Purge section).

#### (U) Disseminating communications involving MCTs

(U//~~FOUO~~) The FAA §702 annual training course, OVSC1203, addresses procedures that analysts must perform for upstream lineage collection containing MCTs comply with the minimization procedures. The training identifies the requirements for disseminating single discrete communication within MCTs. The course also explains requirements for documenting the analysis that supports the decision that communications are eligible before reporting. An NSA reporting policy document, *Source Record Entries for Reporting from FAA 702 Multiple Communications Transaction*, ISS-185-11, requires that compliance be documented in NSA reporting tools. SV performs oversight of the documentation supporting use of certain MCTs for reporting (see the Oversight section).

~~-TOP SECRET//SI//NOFORN-~~

ST-14-0002

**(U) Disseminating attorney-client communications**

**(U//FOUO)** In OVSCJ203, analysts are reminded that the requirement that NSA OGC personnel pre-approve dissemination of information involving USP attorney-client privileged communications.

**(U//FOUO) Disseminating domestic communications** Dissemination of domestic communications is limited to those communications of which DDCRNSA has approved a destruction waiver documenting the illegibility for retention.<sup>88</sup> Such communications must contain information that meets at least one of five criteria: significant foreign intelligence value, technical data, information necessary to assess communications vulnerabilities, evidence of a crime, or information concerning a threat of serious harm to life or property. (Destruction waivers are discussed in the Oversight and Purge sections.) Training on retention and use of domestic communications is included in OVSCJ203.

**(U//FOUO) Disseminating foreign communications affecting USPs**

**(U//FOUO)** OVSCJ203 addresses the requirement to exclude information from reporting that would allow analysts to determine a USP's identity unless the identity qualifies for dissemination under the terms of the FAA §702 minimization procedures. NSA's Information Sharing Services Group (ISS) reviews exceptions to this "masking" requirement. ISS handles requests for release of USP identities.

**(U) Disseminating foreign communications affecting non-USPs** Foreign communications of non-USPs that contain foreign intelligence are eligible for dissemination subject to other applicable laws and policies.

**(U) Dissemination to foreign governments** Information obtained under FAA §702 may be disseminated to foreign governments in three ways (addressed in OVSCJ203):

- [S/SI//REL TO USA, FVEY] [REDACTED] (b)(3)-P.L. 86-36
- [REDACTED]
- [REDACTED]

<sup>88</sup> **(U//FOUO)** A destruction waiver is not required for dissemination of domestic communications to notify the FBI of the target's presence in the United States or to notify the FBI or CIA for collection-avoidance purposes.

~~-TOP SECRET//SI//NOFORN-~~

TOP SECRET//SI//NOFORN

ST-14-0002

(U//FOUO)

(b)(3)-P.L. 86-36

[redacted] Such dissemination must be performed in accordance with special handling procedures and requires the approval of SV and OGC, who maintain records and report this activity to DoJ and ODNI.

~~(S)REL TO USA, FV/HY~~ Dissemination of collection acquired when post-tasking technical checks are not functioning properly In 2013, NSA identified and reported an incident in which a system modification was made to complete production of [redacted] (see the Post-Targeting! (see) in Annex H). Amended minimization procedures approved in November 2003 required application of procedures that NSA developed in response to the incident. These procedures included additional verification of target location before FAA communications acquired during a period when [redacted] post-tasking technical checks are not functioning as intended are used for targeting and dissemination. These procedures were the subject of several communications across SIDs, as well as training sessions, and are documented on NSA's FAA §702 webpage.

(b)(3)-P.L. 86-

(B)(1)  
(b)(3)-P.L. 86-36  
(b)(3)-50 USC 3024(i)

(U//FOUO) Table 35 summarizes the sharing and dissemination provisions of the FAA §702 targeting and minimization procedures and the controls implemented by NSA to maintain compliance.

#### (U) Table 35. Sharing and Dissemination Provisions and Controls

(S)REL TO USA, FV/HY

| Provision  | Control  |
|--|--|
| (U) NSA has established processes to ensure that raw traffic is accessible in authorized repositories only to those who have had the proper training.                                | (U) Annual FAA §702 training addresses analyst responsibility for ensuring that individuals with whom they wish to discuss FAA §702 communications have the necessary credentials and training.  |
| (U) NSA may provide to the CIA and FBI unminimized communications acquired pursuant to FAA §702. These communications will be based upon targets that each agency identifies to NSA. | (S//NF) SV adjudicates TRs from CIA and FBI. If approved, the agencies will receive unminimized communications [redacted]. [redacted] For requested targets whose selectors are already taken by NSA, SID personnel will dual-route [redacted] to provide [redacted] Internet communications to the requesting agency.   |
| (U) Minimization procedures require NSA to be able to purge communications that meet specific requirements.  | (U) To account for and track dissemination based on FAA §702 communications and to comply with purge requirements, analysts must document certain information for the data sources in each report, including the certification under which data was collected and a statement verifying that each piece of traffic used was confirmed as eligible for retention. This is addressed in annual analyst training and NSA reporting policy.<br>(U//FOUO) A new reporting tool, first introduced in 2013, performs the source verification automatically. Successful completion of this |

TOP SECRET//SI//NOFORN

~~TOP SECRET//SI//NOFORN~~

ST-14-0002

|   |   |
|---|---|
|   | process with no flags confirms the traffic is not subject to purge and may be used as a source for reporting.   |
| (U) A dissemination based on communications or concerning a USP that are eligible for retention may be made, if the identity of the USP is deleted and a generic term or symbol is substituted so that the information cannot reasonably be connected with an identifiable USP. Otherwise, dissemination of intelligence based on communications or concerning a USP may only be made to a recipient requiring the identity of such person for the performance of official duties and only if at least one of eight criteria is met.  | (U) This requirement is consistent with NSA reporting policy for all reporting based on communications of USPs.   |
| (U) NSA analysts seeking to use a discrete communication within an MCT for reporting must document that specified analysis has been performed.  | (U//FOUO) Annual FAA §702 training includes the requirements for reporting based upon discrete communications within an MCT and the documentation required. SV reviews this documentation for certain MCTs. (See Oversight - SID Oversight and Compliance.) |
| (U) All proposed disseminations of information constituting USP attorney-client privileged communications must be reviewed by the NSA OGC before dissemination.<br><br>(U) Monitoring of attorney-client communications between a person known to be under criminal indictment in the United States and an attorney representing that individual in the matter under indictment must cease once the relationship has been identified. Acquired communications must be logged and the National Security Division of the DoJ notified so that appropriate procedures may be established to protect such communications from review or use in criminal prosecutions, while preserving foreign intelligence information contained therein.                    | (U) Annual FAA §702 training addresses procedures analysts must perform to disseminate this data. OGC notifies DOJ NSD of such communications and advises mission personnel on dissemination.   |
| (U//FOUO) Minimization procedures require that domestic communications be promptly destroyed upon recognition, unless DIRNSA approves the communication for a destruction waiver. Domestic communications for which a destruction waiver is approved may be disseminated. If a waiver has been obtained, NSA may share domestic communications believed to contain evidence of a crime with appropriate federal law enforcement authorities in accordance with applicable laws and regulations. Without a destruction waiver, NSA is authorized to notify the FBB if information in a domestic communication indicates that a target has entered the United States and may provide information to both the CIA and FBB for collection avoidance purposes. | (U) Annual FAA §702 training addresses this requirement.  |

~~TOP SECRET//SI//NOFORN~~

|  |  |
|--|--|
| (S//REL TO USA, FVEY) NSA is permitted to disseminate evaluated minimized information to foreign partners.   | (S//REL TO USA, FVEY) NSA policy requires that dissemination of EMT acquired pursuant to FAA § 702, other than as serialized product, must be approved by the SIGNNT Director and a record of the dissemination provided to SV.        |
| (U) NSA may disseminate raw data to a foreign government for technical or linguistic assistance.   | (U) Annual FAA § 702 training addresses the requirement that such dissemination must be approved by SV and OGC, who will manage the restrictions on this dissemination, keep the required records, and report to DOD and ODNI.         |
| (S//NF) If NSA seeks to use information acquired pursuant to FAA § 702 when there is uncertainty about the location of the target of the acquisition because [redacted] post tasking checks described in NSA's FAA § 702 targeting procedures were not functioning properly, NSA will follow internal procedures for determining whether such information may be used. | (S//NF) Procedures addressing the requirements for use of data acquired when post tasking [redacted] checks are not functioning as intended were communicated to commission personnel and can be documented on the FAA § 702 web page. |

(S//NF)

(b)(1)

(b)(3)-P.L.866366

**(U) Purge****(U) Background**

(S//REL TO USA, FVEY) The Post-Targeting section documents the requirements for destruction of communications and the processes that may identify a change in the target's location or USP status. These processes include analysis of communications [redacted] and receipt of information from other agencies. If the circumstances result in unauthorized collection, the non-compliant data will be identified and purged.<sup>89</sup> The period of the unauthorized collection is included in an incident report documented by SV and is used by the purge adjudicator, who initiates the purge process.

(U//FOUO) **Compliance controls - purge of FAA §702 communications**<sup>90</sup>

Manual and automated controls support the purge process. SID's Mission Support Systems and Data Compliance Group, within the Directorate for Analysis and Production, developed a purge information web page to guide analysts. This page includes instructions to purge communications collected under FAA §702 authority. The directions call for analysts to contact SV, if they believe that purge of FAA §702 data is required, because analysts assessing purging also require incident reports.

(S//REL TO USA, FVEY) The purge web page describes two types of purges: 1) incident or parametric purges which are necessary when the reason for the purge affects all collection for a target or selector over a period of time (SID's Mission Support Systems and Data Compliance Group performs these); and 2) purge upon

<sup>89</sup> (U) "Purge" refers to the deletion of communications from systems that were acquired as a result of unauthorized collection or otherwise are not authorized for retention pursuant to the minimization procedures.

<sup>90</sup> (S//SI//NOFORN) From the time of collection, [redacted]

[redacted] The following description focuses on the [redacted]

~~TOP SECRET//SI//NOFORN~~

ST-14-0002

recognition or analyst-driven purges. A parametric purge is applied, for example, to remove communications collected after a target is determined to be in the United States. Purge upon recognition for FAA § 702 is, for example, required when: 1) NSA identifies a discrete domestic communication within an MCT, requiring the entire MCT to be purged or 2) a legally acquired foreign communication between a foreign target and a USP or a communication in which the subject is a USP found to have no foreign intelligence value.

(U//~~FOUO~~) NSA has implemented admission compliance standards for purges which states that, consistent with NSA's FAA § 702 minimization procedures and absent a destruction waiver, some or all communications data acquired under the authority must be purged if any of the following criteria are satisfied:

- (U) The targeted person is confirmed or believed to be a USP, regardless of location (purge all communications),
- (U) The targeted person was confirmed or believed to be in the United States at the time of collection (manner) (purge collection acquired during period of U.S. travel),
- (U) A person was incorrectly targeted (purge all collection),
- (U) The tasked selector is known or suspected to be used by a USP (purge all communications from known date of use by the USP),<sup>91</sup>
- (U) The tasked selector was known or suspected to be accessed from within the United States (purge communications from date of access),
- (U) The tasked selector was tasked before being approved for tasking, remained tasked for any reason after collection was no longer authorized, or was tasked under the wrong authority (purge all collection),
- (U) An incorrect selector was tasked (purge all collection),
- (U) The communication is one in which the sender and all intended recipients were in the United States at the time of acquisition of the communication (purge affected communications), or
- (U//~~FOUO~~) The communication otherwise qualifies as "domestic communication" as defined in the FAA § 702 minimization procedures and DIRNSA or the Acting DIRNSA has not executed a destruction waiver to authorize continued retention of the communication (purge affected communications).

(U//~~FOUO~~) **Purge processes** Purging involves four processes: nominate data to purge, adjudicate purge nominations, execute purge actions, and verify purge actions. Other systems are certified to hold certain data copied or derived from [redacted] data

(b)(3)-P.L. 8636

<sup>91</sup> (SINR) [redacted]

(b)(3)-P.L. 8636

(b)(3)-P.L. 8636

~~TOP SECRET//SI//NOFORN~~

TOP SECRET//SI//NOFORN

ST-14-0002

objects. These systems have their own purge processes. The following description focuses on the [redacted] (b)(3) P.L. 86-36

(U//FOUO) **Nomination for purge** Nomination involves identification of the selectors and time period of communication that needs to be destroyed. For FAA §702, most are identified in incident reports, and SV determines whether purge is required and documents the date range of purge in the incident report. Purges of specific data objects are also initiated by analysts recognizing content that meets minimization criteria, but which is not an indicator of a compliance incident. This process is known as "purge upon recognition." For this type of purge, the identifiers of the affected communications are placed in the MPL "discover state" before a modified version of the process described below is followed.

(U//FOUO) **Adjudicating purge nominations** Purge adjudication is the process whereby the purge adjudication authority, SDD's Mission Support Systems and Data Compliance Group, determines the validity and accuracy of a nominated purge request, locates the data required for destruction, and places the data objects in the master purge list (MPL). The goal of adjudication is to ensure compliance with purge criteria without over purging communications at the expense of mission. The adjudicator:

- (U//FOUO) Evaluates the nomination against the purge criteria (unless a determination was made during initial processing).
- (U//FOUO) Using logical parameters provided in the nomination, determines and issues search criteria for discovery of potentially affected communications in the [redacted]<sup>92</sup>
- [redacted]
- (U//FOUO) Enters identifiers of affected data objects in the MPL in "discover state" to prevent use as a source for new SIGINT reporting or other controlled uses and to initiate checks to determine if the objects were used in prior SIGINT reporting.
- (U//FOUO) Manages the impact of pending or approved destruction waivers that may exclude specific objects from purge.
- (U//FOUO) For data objects requiring purge, changes MPL state of their identifiers to "purge" and issues purge execution orders to the [redacted] to delete those objects, and
- (U//FOUO) Records the decision to purge, release, or quarantine the data objects in the corporate purge tracking system, [redacted] which retains (b)(3) P.L. 86-36

<sup>92</sup> (U//FOUO) The discovery process is performed by a limited number of individuals with special access for each [redacted]

TOP SECRET//SI//NOFORN

TOP SECRET//SI//NOFORN

ST-14-0002

submitted data identifiers with historical records of actions taken and cross-references to original compliance incidents and/or purge nominations that caused them to enter the purge process.

(U//~~FOUO~~) For purges stemming from system or technical errors, collection and/or technical subject matter experts are typically relied upon to conduct or assist with purge discovery. Some aspects of the adjudication process may be modified based on the details of the specific incident.

(U//~~FOUO~~) **Executing purge actions** The purge executor receives purge decisions from the adjudication authority, issues execute orders to [redacted] system Owners containing the unique identifiers of the data to be purged, confirms receipt of the orders, changes the MPL status of those identifiers to "purge," and retains records of the purge action for five years. [redacted] system owners are responsible for processing the orders, rendering the specified data unrecoverable, and confirming completion of purge execute orders. (b)(3)-P.L. 86-36

(U//~~FOUO~~) **Verifying purge actions** Procedures are performed to provide additional assurance that system owners have purged required SIGINT data from NSA [redacted] 1. SV obtains random samples of data from the master purge list and determines whether the data objects have been removed from the systems selected for review.

(U//~~FOUO~~) **Automation to support purge processing** Much of the purge process is performed manually. NSA is developing a system to automate more of the purge process in phases between [redacted]. (b)(3)-P.L. 86-

(U//~~FOUO~~) **Reports affected by purge actions** SIGINT reporting procedures require MPL checks to prevent publication of new reports with sources that were subject to purge. Additional measures are taken to detect and adjudicate already-disseminated SIGINT products affected by a compliance incident or specific data identified during purge discovery. Incident reports include information SV obtained from the mission team on reports issued related to the target or collection referenced in the incident. Another source of information is a daily query run by NSA's management information systems (MIS) against the MPL to identify reports sourced from communications listed on the MPL, whether because of an incident or purge upon recognition.

(U//~~FOUO~~) When SIGINT products with potentially tainted sources are identified, the Reports under Review (RUR) team coordinates with the mission team that issued the report, the purge adjudication authority, SV, and OGC, as necessary, to determine and complete appropriate actions. This may include requesting a destruction waiver to permit retention of the traffic and allowing the report to stand, removing the MPL-listed traffic completely from the report and revising and reissuing the report or recalling the report. The RUR team maintains a list of affected reports and their status that is updated without the report analysis is complete. The purge adjudication

TOP SECRET//SI//NOFORN

authority makes necessary changes to the status of the communication identifier on the MPL, depending on the action taken.

(U//FOUO) Table 36 summarizes the purge provisions of the FAA §702 targeting and minimization procedures and the controls NSA has implemented to maintain compliance.

**(U) Table 36. Purge Provisions and Controls**

(S//NF)

| Provision   | Control  |
|---|--|
| (U//FOUO) Telephony communications and Internet communications acquired with the assistance of the FBI from Internet service providers that are not approved for retention under the standards set forth in the minimization procedures and that are known to contain communications of or concerning USPs will be destroyed upon recognition.  | (U//FOUO) Annual FAA §702 training addresses post-targeting review of target communications and situations requiring destruction of communications, which most often require notification to SV and an incident report.  |
| (U//FOUO) Internet transactions acquired through NSA's upstream collection techniques that do not contain information that meets the retention standards set forth in the minimization procedures and that are known to contain communications of or concerning USPs will be destroyed upon recognition.  | (U//FOUO) Annual FAA §702 training addresses post-targeting review of target communications and situations requiring destruction of communications, which most often require notification to SV and an incident report.  |
| (U) Internet transactions that are identified and segregated pursuant to the requirements for processing MCTs and are subsequently determined to contain a discrete communication in which the sender and all intended recipients are reasonably believed to be in the United States will be handled as domestic communications.  | (U//FOUO) Annual FAA §702 training addresses post-targeting review of target communications and situations requiring destruction of communications, which most often require notification to SV and an incident report.  |
| (U//FOUO) A communication identified as a domestic communication (and, if applicable, the Internet transaction in which it is contained) will be promptly destroyed upon recognition, unless DIRNSA or the Acting DIRNSA approves a destruction waiver after determining the communication meets one or more of four specific conditions.   | (U//FOUO) Annual FAA §702 training addresses post-targeting review of target communications and situations requiring destruction of communications, which most often require notification to SV and an incident report.  |
| (U//FOUO) Any communications acquired through the targeting of a person who at the time of targeting was reasonably believed to be outside the United States but is in fact inside the United States at the time such communications were acquired and any communications acquired by targeting a person who at the time of targeting was believed to be a non-USP but was in fact a USP at the time such communications were acquired will be treated as domestic communications under these procedures. | (U//FOUO) Annual FAA §702 training addresses post-targeting review of target communications and situations requiring destruction of communications, which most often require notification to SV and an incident report.<br><del>SHRED TO USA, PIVET</del> In addition to analysis review of communications, investigation of [redacted] notices from others involved in processing FAA §702 information, and receipt of information from other agencies may identify an incident. If the circumstances of the collection require an incident report, analysts and SV work together to determine the extent of the communications affected. This is used to document the purge parameters in an |

TOP SECRET//SI//NOFORN

ST-14-0002

|  |   |
|--|---|
|  | <p>incident report, which becomes the source for the purge adjudication process.</p> <p>(U//FOUO) Communications identified for purge are subject to adjudication to determine whether the nominated data objects are consistent with the purge criteria; communications affected by the incident have been properly identified; destruction waivers (pending or approved) may affect the purge.</p> <p>(b)(3)-P.L. 86-36</p> <p>[ ] The adjudicator adds the relevant data to the Master Purge List (MPL) to prevent its use in targeting and reporting and issues purge execute orders to appropriate systems.</p> <p>(U//FOUO) Owners of the FAA §702 [ ] execute the purge orders, remove data matching the included identifiers, and acknowledge completion of each order.</p> <p>(U//FOUO) NSA's management information system for SIGINT reporting queries the MPL daily to identify data objects added to the list that may be associated with issued reports. The Reports Under Review team uses this information and incident report data concerning reporting associated with the affected communications to follow up with mission personnel for recall or reissuance of the reports.</p> <p>(U//FOUO) SV randomly samples records from the MPL, comparing them to the FAA §702 repositories to assure completeness of purge.</p> |
| <p>(S//NF) For information acquired pursuant to FAA §702 during a period where [ ] post-tasking checks were not functioning properly, resulting in uncertainty about the location of the target of the acquisition, if NSA determines that the target is reasonably believed to have been inside the United States at the time the information was acquired, such information will not be used and will be promptly destroyed.</p> | <p>(S//NF) SID guidance, NSA Procedures for the Use of FAA 702 7004 or 705(h) Collection last revised 15 November 2013, was updated to provide manual procedures for evaluating data when NSA's post-tasking [ ] checks are not properly functioning.</p> <p>(b)(1)</p> <p>(b)(3)-P.L. 86-36</p>  |

(S//NF)

### (U) Retention of Data

#### (U) Provisions of FAA §702 certifications

(U//FOUO) The retention criteria in the minimization procedures apply only to communications not subject to purge based upon other minimization requirements (see the Post-Targeting section).

(U//FOUO) NSA minimization procedures state that telephone [ ] communications will be retained no longer than five years from the expiration date of the certification authorizing collection, unless NSA analysts have determined that the communications meet the retention standards set forth in the minimization procedures, for example, communications necessary to understand foreign intelligence information. Communications for which SIDDIR has approved longer retention and for which a purge waiver or otherwise qualified analysis can be attached.

(b)(3)-P.L. 86-

TOP SECRET//SI//NOFORN

Communications for which DIRNSA has waived destruction may also be retained in accordance with the terms of the destruction waiver.

(U) In general, NSA may not retain Internet transactions obtained through upstream collection techniques longer than two years from the expiration date of the certification authorizing collection. However, NSA may be able to retain certain Internet transactions longer if at least one discrete communication within the upstream Internet transaction would otherwise meet the retention standards and each discrete communication within the transaction is to, from, or about a tasked collector or not to, from, or about a tasked collector and is also not to or from a USP or person reasonably believed to be in the United States. The minimization procedures also required destruction of all upstream Internet transactions acquired before November 2011.

#### **(U) Retention control procedures**

(U//~~FOUO~~) **System certification** The NSA system certification process implemented in 2010 (see the Repositories section) includes the Agency's requirements for compliance with the FAA §702 retention limits established in the minimization procedures. To be certified, FAA §702 systems must: 1) limit retention of unminimized data records to the authorization and retention periods of the certification under which they were collected, 2) retain data with an approved age-off waiver beyond the normal age-off period (SID Director waiver), and 3) provide a means to identify data records to be retained beyond the maximum retention period specified by the collection authority under which it was obtained.<sup>93</sup>

(U//~~FOUO~~) **Data tagging** Data tags are now associated with most collection before it is made available to data stores accessible to analysts. The tags include the certification under which the communications were obtained, further supporting NSA's ability to identify records that meet the criteria for removal from system repositories based upon age-off requirements associated with each certification. In 2014, new data tags were implemented to distinguish among the retention periods for upstream Internet transactions (two years), downstream collection (five years) and telephony data (five years).

(U//~~FOUO~~) **Implementation and monitoring page off** Processes have been implemented to age-off data in FAA §702 [REDACTED]. Though the minimization procedures require data be aged-off within two or five years of expiration of the certification, depending upon the source of collection, the processes NSA uses for determining age-off result in earlier removal of data (see Table 37).<sup>94</sup>

(b)(3)-PL-866366

<sup>93</sup> (U//~~FOUO~~) NSA's FAA §702 minimization procedures provide no maximum retention period for foreign communications determined to contain foreign intelligence information. The age-off requirements apply to communications for which such a determination has not been made.

<sup>94</sup> (U//~~FOUO~~) The FAA 702 certifications are renewed annually. Expiration of the certification effect for any collection would occur somewhere between 1 and 365 days of that collection. NSA applies age-off criteria to time of collection or recording date, not the expiration of the certification.

~~TOP SECRET//SI//NOFORN~~

ST-14-0002

(b)(3)-P.L. 86-36

(U) Table 37. System Age-Off Procedures

| (TS//SI//NF)  | Upstream Procedure for Data Age-Off | Telephony and downstream Internet Collection Procedure for Data Age-Off | Monitoring for Compliance with Age-Off Criteria |
|---|-------------------------------------|---|---|
| r [redacted]  |                                     |   |   |
| <p>(b)(11)<br/>           (b)(3)-P.L. 86-36<br/>           (b)(3)-50 USC 3024(ii)</p> <p>* (U//FOUO) Enterprise data header (EDH) is a small set of metadata tags applied to a piece of mission data so that it can be identified, protected, tracked, and handled throughout its lifecycle. [redacted] will only accept data with an EDH.</p> <p>† (U//FOUO) Systems scheduled to be decommissioned.</p> <p>‡ (U//FOUO) PDCO data at time of intercept.</p> <p>§ (TS//SI//NF) [redacted]<br/> [redacted]<br/> [redacted]</p> |                                     |   |   |
| (TS//SI//NF)  |                                     |   |   |

(b)(3)-P.L. 86-36

(b)(11)  
(b)(3)-P.L. 86-36

(U//FOUO) Table 38 summarizes the retention provisions of the FAA §702 targeting and minimization procedures and the controls NSA implemented to maintain compliance.

~~TOP SECRET//SI//NOFORN~~

## (U) Table 38. Retention Provisions and Controls

(U//FOUO)

| Provision  | Control  |
|--|--|
| (U) Telephony communications and Internet communications acquired by or with the assistance of the FBI from Internet Service Providers may not be retained longer than five years from the expiration date of the certification authorizing the collection unless NSA determines that each communication meets the retention standards in these procedures.  | (U) System certification, required of all FAA §702 systems, includes retention standards consistent with minimization procedures.<br>(U) Data tags are now associated with most collection before it is made available to data stores accessible to analysts. Data tags support identification of records for age-off.   |
| (U) Internet transactions acquired through NSA's upstream collection may not be retained longer than two years from the expiration date of the certification authorizing the collection, unless NSA determines that each communication meets the retention standards in these procedures.<br>[Additional requirement regarding MCCTs are addressed in the Purge section.]  | (U//FOUO) [REDACTED] utilizes a software tool to search for data beyond the required age-off procedure. A similar tool is being developed for [REDACTED].  |
| (U) Internet transactions that are identified and segregated pursuant to the procedures for MCCTs will be retained in an access-controlled repository.<br>(U) Any information contained in a segregated Internet transaction may not be moved or copied from the segregated repository or otherwise used for foreign intelligence purposes unless it has been determined that the transaction does not contain any discrete communication as to which the sender and all intended recipients are reasonably believed to be located in the United States. | (U//FOUO) NSA has implemented a segregation process and sequestered MCCT data is maintained in a collection store where it is not available for analytic use. None of the data subject to sequestration has been transferred to repositories accessible to analysts.<br>(U//FOUO) NSA has deleted all identified upstream Internet collection acquired before November 2011. If additional data is identified that was subject to this purge requirement, NSA deletes it upon recognition. |
| (U) Any Internet transactions acquired through NSA's upstream collection techniques prior to 31 October 2011 will be destroyed upon recognition..  | (U//FOUO) (b)(3)-P.L. 86-36<br>(U) These controls are documented in the Collection section.  |

(U//FOUO)

## (U) Oversight

## (U) Provisions of FAA §702 certifications—internal and external oversight

(U//FOUO) The FAA §702 targeting and minimization procedures provide that NSA will conduct the following oversight:

- (U) Implement a compliance program with ongoing oversight of its exercise of FAA §702 authority, including the associated targeting and minimization procedures
- (U) Develop and deliver training regarding procedures to ensure that intelligence personnel responsible for approving targeting of persons under these procedures, as well as analysts with access to the acquired foreign intelligence information, understand their responsibilities and the procedures that apply to this acquisition

~~TOP SECRET//SI//NOFORN~~

ST-14-0002

- (U) Establish processes for ensuring that raw traffic is labeled and stored only in authorized repositories and is accessible only to those who have had the proper training
- (U//FOUO) Conduct ongoing oversight activities and make necessary reports to the NSA OIG and OGC, including reports of non-compliance
- (U) Ensure corrective actions are taken to address identified deficiencies
- (U) Conduct periodic spot checks of targeting decisions and intelligence disseminations to ensure compliance with established procedures and conduct periodic checks of queries in data repositories
- (S//NF) Report incidents of non-compliance with the targeting and minimization procedures within five business days of discovery to the DoJ NSD and ODNI's oversight team.<sup>95</sup>

(U) DoJ NSD and ODNI oversight requirements include:

- (U) Oversee NSA's exercise of the FAA §702 authority, including bi-monthly reviews to evaluate the implementation of the procedures
- (U) Oversee NSA's activities with respect to use of USP identifiers to query communications collected under FAA §702.

(U) **NSA oversight**

(U//FOUO) NSA operates a comprehensive oversight framework to maintain compliance with the FAA §702 targeting and minimization procedures. The NSA organizations that perform oversight are described below.

(U//FOUO) **FAA §702 Authority Lead** is responsible for the implementation and operation of the FAA §702 authority for NSA. The FAA §702 Authority Lead serves on NSA's corporate Authorities Integration Group and works with other NSA mission Authority Leads and corporate legal, policy, compliance, and technology personnel to coordinate implementation of NSA mission authorities. The FAA §702 Authority Lead addresses the tactical and strategic elements of the program; interacts regularly with NSA's OGC, ODOC, TD, LAO, and SDD; routinely interacts with DoJ NSD, ODNI, HEBI, and CIA; provides direction regarding daily operational and technical questions; and coordinates input to reports to Congress and the HISAC Comittee.

(U//FOUO) **Authorities Integration Group (AIG)** is administratively assigned to ODOC and reports to the NSA Deputy Director. The AIG works directly with SDD and Information Assurance Directorate authority leads, including the FAA §702 Authority Lead, and holds weekly meetings with the authority leads and corporate process leads (e.g., TD, ODOC, OGC) to bring legal, policy, compliance, technology, and mission areas together to provide recommendations on the implementation of the

<sup>95</sup> (U) ODNI's oversight team is comprised of ODNI's Office of General Counsel, ODNI's Civil Liberties and Privacy Office, and ODNI's Office of the Deputy Director of National Intelligence for Intelligence Integration/Mission Integration Division.

~~TOP SECRET//SI//NOFORN~~

authorities. The AIG focuses on the activities of each authority, internal and external, to ensure that they are coordinated and integrated across NSA. The AIG acts as a "forcing function" within NSA, facilitating discussion among the Directorates to promote better understanding of how decisions affect the various authorities. The AIG updates the NSA Deputy Director quarterly on each authority.

(U//FOUO) Office of the Director of Compliance (ODOC) is responsible for developing and directing the execution of compliance strategies and activities focused on protecting USP privacy during the conduct of authorized NSA missions. ODOC has the authority to develop, implement and monitor the Comptroller's Mission Compliance Program for the Agency, which addresses (1) integration of compliance strategies and activities across NSA mission technology and policy organizations; (2) a training and education program for compliance; and (3) maintenance of and reporting on the status of mission compliance. The CMCP's focus is on mission compliance, particularly in Signals Intelligence and Information Assurance operations, including the technology by which they conduct their objective. The objective of the CMCP is to provide reasonable assurance that the legal authorities and policies affecting USP privacy are reliably and verifiably followed by NSA. The CMCP includes activities and funding to support compliance with FAA § 702, such as compliance target validation and query symbols.

(U//FOUO) ODOC's monitoring activities provide continuous assessment to determine whether internal controls are operating as intended. Its assessment helps management evaluate the effectiveness of the compliance program and its components. For example, ODOC reviews compliance activities associated with queries in NSA repositories, including those related to FAA § 702:

- (U//FOUO) ODOC analyzes [redacted] queries ...W... (b)(3)P.L. 86-36 forwarded to the privacy audit database that could indicate a problem in communicating with the repositories queried,
- (U//FOUO) It verifies that all queries requiring post-query review are assigned to reviewers,
- (U//FOUO) It monitors the number of queries selected for review and the timeliness of review, and
- (U//FOUO) It tracks the supervisory performance by SV (see the Oversight section).

(U//FOUO) In addition, ODOC performs Compliance With Availability Discovery (CVD) reviews that focus on high-risk areas within the CMCP to discover compliance weaknesses. In 2013, ODOC completed two CVDs focused on mission compliance with SIGNINT authorities. Table 39 summarizes these CVDs.

~~TOP SECRET//SI//NOFORN~~

ST-14-0002

## (U) Table 39. Compliance Vulnerability Discovery Reviews

(Unrefined)

| Date Issued | SIGINT Authority | CVD Review                               | Scope of the Review  |
|-------------|------------------|--|--|
| 05/03/13    | FISA/FAA §702    | Multiple Communications Transactions     | Reviewed implementation of controls to segregate unauthorized data from NSA's FAA §702 Upstream Multiple Communications Transactions |
| 07/17/13    | All              | Data Tagging<br>[redacted]<br>[redacted] | Reviewed data from NSA systems for proper tagging to support designation of these systems as [redacted]                              |

(b)(3)-P.L.866386

(U//FOUO)

(U//FOUO) ODOC has also implemented processes to ensure that NSA representations to external overseers are accurate and NSA personnel have a consistent understanding of program activities. VoA and verification of implementation reviews are performed on written NSA representations that describe the Agency's acquisition, processing, retention, analysis, and dissemination of information for legal opinions, FISC Orders, and Executive Branch decisions. In 2013, ODOC conducted VoAs with FAA §702 stakeholders for the affidavits and targeting and minimization procedures supporting renewals of FAA §702 certifications. One verification of implementation was conducted in June 2013 with NSA's external partners (DOD NSD and ODNI) on procedures for implementing the FAA §702 targeting procedures.

(U//FOUO) SV implements the SIGINT compliance program across NSA. SV establishes SIGINT compliance standards and provides guidance across the global SIGINT enterprise, manages incidents of non-compliance, monitors compliance in high risk areas, resolves problems, and verifies compliance through audits by managing the SIGINT Intelligence Oversight Office program. SV manages resources to ensure that NSA corporate systems and capabilities align with CMCP solutions.

~~(C/REL TO USA, FVEY)~~ To maintain NSA's compliance with the FAA §702 targeting and minimization procedures, SW:

- (S/NF) [redacted]
- (S/NF) [redacted] 1 [redacted]
- (U//FOUO) Adjudicates TRs for selectors nominated by the CIA and FBI, utilizing the same process used for NSATRs [redacted]
- (S/REL TO USA, FVEY) Performs post-tasking analysis for FAA §702 selectors suspected of being accessed within the United States [redacted]

~~TOP SECRET//SI//NOFORN~~

- (U//~~FOUO~~) Investigates all incidents of non-compliance with FAA §702 targeting and minimization procedures, coordinating with TV when a potential incident involves a system. SV works with the mission team to document FAA §702 incidents, promptly reports them to OGC, OIG, and ODNI, and maintains a permanent record.
  - (U//~~FOUO~~) Works with mission personnel and OGC to process destruction waivers as needed.
  - (U//~~FOUO~~) Conducts super audits of queries of raw SIGINT databases that provide records of queries to the corporate logging and auditing system to analyze the quality of query reviews by auditors.
  - (U//~~FOUO~~) Completes Punge Verification Activities quarterly for [redacted] and certain other stores that hold FAA §702 data to assess NSA's effectiveness in purging non-compliant SIGINT. (b)(3)-P.L. 86-36
  - (U//~~FOUO~~) Oversees use of MCTs as a source for reporting and verifies completion of required documentation.<sup>96</sup>
  - (U//~~FOUO~~) Serves as the FAA §702 tasking liaison for the NSA Enterprise, IC customers (FBI and CIA), and overseers from DoJ NSD and ODNI.
  - (U//~~FOUO~~) Provides documentation for review by DoJ NSD and ODNI. SV reviews [redacted] for each selector tasks and reviews records of information shared with NSA's R&D partners for compliance with dissemination requirements. Records of database queries using USR query terms and records of USP reporting are also provided to overseers. SV coordinates responses by NSA organizations to questions from DoJ NSD and ODNI during their review of information SW made available.
  - (U//~~FOUO~~) Pre-approves USP content queries in conjunction with OGC.
  - (U//~~FOUO~~) Participates in the verification of accuracy process for renewals of certifications and targeting and minimization procedures.
  - (U//~~FOUO~~) Partners with the Associate Directorate for Education and Training to develop and implement oversight and compliance training for the SIGINT workforce. SV co-develops and reviews all updates of the FAA §702 course.
- (U//~~FOUO~~) SID Analysis and Production, Mission and Compliance Office This office supports all areas of NSA's SIGINT operations by overseeing:

<sup>96</sup> (S//NF) Three types of MCTs are made available to analysts. Two types of transactions made available to analysts after the MCT sequestration process are those that contain only discrete communications (no MCTs) and those where the active user of the selector is a targeted individual. SV performs oversight of the third type, where the active user of the selector is a non-targeted individual outside the U.S. (an example of "abouts" collection). SV examines these MCTs for compliance with NSA reporting guidance (ISS-185-11), which states that analysts are "only authorized to use those discrete portions of MCTs containing the targeted selector."

~~TOP SECRET//SI//NOFORN~~

ST-14-0002

- (U//~~FOUO~~) FAA §§702 adjudication and training (interfacing with analysts on how to use the authority, approving new adjudicators who receive training and mission requirements, and reviewing adjudicated TRRs for compliance)
- (S//~~REL TO USA, FVEY~~) Dual-route adjudication (approving provision of the results of targeting to the CIA or FBI forst letters already on NSA collection)
- (S//~~REL TO USA, FVEY~~) FISA and production metrics (providing feedback to management on use of the authority and analyst/adjudicator performance)
- (S//~~REL TO USA, FVEY~~) The application of the authority (e.g., instructions for maintaining compliance when [redacted] were not operating, targeting and adjudication checklists, and general guidance on the analytic use of the authority).

(b)(f)  
(b)(3)-P.L.886386

(U//~~FOUO~~) TD Office of Compliance (TV) is responsible for identifying, assessing, tracking, and mitigating compliance risks, including USIS Privacy concerns in NSA mission systems across the enterprise, including systems that hold PAAA §702 data. TV manages the system compliance certification process, continuous compliance monitoring, and technical compliance incident reporting and also trains technical personnel. TV performs VoAs for areas assigned to it in NSA representations.

(b)(3)-P.L.886386

(U//~~FOUO~~) [redacted] TV began certifying HSAs systems, including the FAA §§702 systems, to ensure compliance with the law and policies protecting USIS privacy (see the Repositories section).

(U) The Office of the General Counsel provides legal advice to NSA and is the liaison to DoJ NSD for NSA's FAA §702 program. One of its main oversight responsibilities involves independently assessing potential incidents of non-compliance.

(U) OGC receives reports of potential incidents of non-compliance from SW. OGC compiles FAA §702 incidents daily, provides them to DoJ NSD and ODNI, and makes an initial determination whether incidents represent non-compliance with the FAA §702 certifications and targeting and minimization procedures. OGC notifies DoJ NSD and the ODNI's oversight team of potential incidents of non-compliance with the targeting procedures within five business days of discovery, as FAA §§702 targeting procedures require. OGC reviews all proposed disseminations of information constituting USIS attorney-client privileged communications before dissemination, as NSA's FAA §702 minimization procedures require. For all violations of NSA's FAA §702 targeting and minimization procedures, OGC coordinates input from NSA organizations and edits the content of a factual and legal accuracy. DoJ NSD prepares Rule 13 notices, in coordination with ODNI.

~~TOP SECRET//SI//NOFORN~~

(U) OGC performs additional oversight responsibilities including:

- (U//~~FOUO~~) Reviews requests to perform content queries using USP selection terms. Only OGC approved selection terms can be used to perform content queries of USP information.
- (S//NF) [REDACTED]
- (S//NF) [REDACTED]
- (TS//SI//NF) Reviews tasking [REDACTED]
- (S//NF) [REDACTED]
- (U//~~FOUO~~) Participates in the VoA process.
- (U//~~FOUO~~) Reviews and makes updates to the FAA §702 course, as necessary.

(U) Office of the Inspector General (OIG) conducts audits, special studies, inspections, investigations, and other reviews of the programs and operations of NSA and its affiliates. OIG oversight includes:

- (U) Performing audits and special studies of the FAA §702 program
- (U) Receiving notification of incident reports for all NSA authorities, including HAAA §702, saved in the Agency's corporate incident reporting database
- (U//~~FOUO~~) Reviewing Congressional notifications and notices filed with the FISC of incidents of non-compliance with HAAA §702 targeting and minimization procedures
- (U) Preparing Intelligence Oversight Quarterly Reports, in coordination with the DIRNSA and OGC, that summarize compliance incidents for all authorities occurring during quarterly review periods and forwarding the reports to the President's Intelligence Oversight Board through the ATSD(IO)<sup>97</sup>
- (U) Performing intelligence oversight reviews during OIG inspections of joint and field sites
- (U) Maintaining the OIG Hotline, responding to complaints, including allegations of SIGINT misuse by NSA affiliates operating under DIRNSA's authority
- (U) Reporting immediately to the ATSD(IO) a development or circumstance involving an intelligence activity or intelligence personnel that could impugn the reputation or integrity of the IC or otherwise call into question the propriety of an intelligence activity.

(b)(1)  
(b)(3)-P.L. 86-36  
(b)(3)-50 USC 3024(i)

<sup>97</sup> (U//~~FOUO~~) In 2014, the ATSD(IO) was changed to the Office of the Senior DoD Intelligence Oversight Official.

~~-TOP SECRET//SI//NOFORN-~~

ST-14-0002

(U//~~FOUO~~) The OIG reviews management controls, maintains awareness of compliance incidents, and stays informed of changes affecting NSA authorities, including FAA §702. OIG reviews of the FAA §702 program allow it to independently assess compliance with minimization procedures. Since the Agency obtained FAA §702 authority in January 2008, the OIG has completed annual reviews of reports containing references to USP identities and targets later determined to be in the United States, as the statute requires. The OIG has also completed two special studies of the program (Table 40).

(U) Table 40. OIG Reviews of the FAA §702 program

| (S//NF) | Date Issued | OIG Review  | Scope of the Review  |
|---------|-------------|---|--|
|         | 3/29/13     | (U) Assessment of Management Controls Over FAA §702 (SFT-1-00099) | (U// <del>FOUO</del> ) Reviewed management controls for maintaining compliance with targeting and minimization procedures. |
|         | 10/29/13    | (S//NF)   | (S//NF)  |

(b)(1)

(b)(3)-P.L.866386

(U) External oversight (b)(3)-50 USC 3024(i)

(S//NF)

(U//~~FOUO~~) DoJ NSD and ODNI closely coordinate to perform oversight to ensure that NSA's FAA §702 program is compliant with the statute and FISC rulings. DoJ NSD is the primary liaison between NSA and the FISC for all matters pertaining to the FAA §702 program. DoJ NSD and ODNI oversight includes:

- (U//~~FOUO~~) Reviewing and approving annual certification renewals and updates of the associated targeting and minimization procedures and filing them for FISC approval
- (U) Providing guidance to the NSA OGC on legal opinions relating to the interpretation, scope, and implementation of the FAA §702 authority
- (U//~~FOUO~~) Reviewing briefings on NSA proposals to substantially modify systems or processes supporting FAA §702. This allows NSD to determine that the modifications are lawful and that the Attorney General (AG) and the FISC are aware of the scope and nature of the changes
- (U) Evaluating and investigating potential incidents of non-compliance with the statute or procedures and reporting any matter determined to be a compliance incident to the FISC
- (U) Reviewing NSA briefings and training transcripts to ensure that they accurately describe the requirements of the FAA §702 Orders
- (S//NF) Performing bi-monthly reviews of NSA authorities under the [redacted] FAA §702 certifications. The reviews include NSA's targeting decisions,

(b)(1)

(b)(3)-P.L.866386

(b)(3)-50 USC 3024(i)

~~-TOP SECRET//SI//NOFORN-~~

including source documentation supporting these determinations, to assess compliance with NSA targeting procedures and AG Acquisition Guidelines. The reviews also examined databases querying USP query terms and disseminations of serialized reporting and EWIT.

- (U) Preparing the periodic reports the statute requires:

1. (S//NF) DoJ submits the *Semiannual Report of the AG Concerning Acquisitions under Section 702 of the FISA* to Congress and the FISC.

Pursuant to FISA §707, the AG reports on the acquisition of foreign intelligence information conducted under the [REDACTED] FAA §702 certifications by NSA and FBI. While the CIA does not acquire the information, it may receive unminimized data that NSA and FBI acquired. The AG's semiannual reports focus on analysis of incidents of non-compliance with targeting and minimization procedures by NSA and FBI and incidents of non-compliance with minimization procedures by CIA.

2. (S//NF) Jointly, the AG and the DNI submit the *Semiannual Assessments of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the FISA* to Congress and the FISC. These reports summarize the oversight performed on implementation of the FAA §702 authority, trends in targeting and minimization (e.g., changes in the number of selectors wider collection and statistics on use of the [REDACTED] certifications), and compliance incidents with the FAA §702 authority for NSA, FBI, and the CIA.

- (U) ODNI hosts bi-monthly interagency meetings and a weekly phone call to discuss FAA §702 implementation and compliance matters.

(S//NF) The FISC reviews and, when satisfied that the legal requirements have been met, approves all renewals of certifications and targeting and minimization procedures for the FAA §702 authority that have been authorized by the AG and DNI.<sup>98</sup> In addition, the FISC reviews representations NSA made regarding the operation of the program and Rule 13 notices of incidents of non-compliance filed by DoJ NSD on behalf of NSA. If the Court finds that incidents of non-compliance result from processes inconsistent with the targeting and minimization procedures (e.g., incomplete application of the [REDACTED] identification), NSA will be required to change its internal systems or procedures and report to the Court on the progress made to achieve compliance. The Court may also determine that additional measures or changes are required to the targeting and minimization procedures (e.g., sequestration of MCTs), if it deems that NSA processes do not adequately protect USPs.

(b)(1)  
(b)(3) P.L. 86-36  
(b)(3) 50 USC 3024(i)

<sup>98</sup> (U//FOUO) The AG and DNI authorize the collection of data pursuant to FAA §702 using targeting and minimization procedures adopted by the AG (in consultation with the DNI). The FISC must approve the certifications and associated procedures that the AG and DNI have authorized.

~~TOP SECRET//SI//NOFORN~~

ST-14-0002

(U//~~FOUO~~) Table 41 summarizes the oversight provisions of the FAA §702 targeting and minimization procedures and the controls NSA implemented to maintain compliance.

(U) **Table 41. Oversight Provisions and Controls**~~(S//NF)~~

| Provision  | Control   |
|--|---|
| (U) NSA will implement a compliance program, and will conduct ongoing oversight, with respect to its exercise of the authority under FAA §702, including the associated targeting and minimization procedures.   | (U// <del>FOUO</del> ) NSA operates a comprehensive oversight framework to maintain compliance with the FAA §702 targeting and minimization procedures. This compliance framework is collectively managed by the NSA organizations described above.   |
| (U) NSA will develop and deliver training regarding the applicable procedures to ensure intelligence personnel responsible for approving the targeting of persons under these procedures, as well as analysts with access to the acquired foreign intelligence information, understand their responsibilities and the procedures that apply to this acquisition. | (U// <del>FOUO</del> ) SV partners with the Associate Directorate for Education and Training to develop and implement oversight and compliance training for the SIGINT workforce. SV co-developed and reviewed all updates of the FAA §702 course. OGC also reviews and updates the FAA §702 course.  |
| (U) NSA will establish processes for ensuring that raw traffic is labeled and stored only in authorized repositories and is accessible only to those who have had the proper training.   | (U// <del>FOUO</del> ) TV certifies NSA systems periodically, including the FAA §702 systems, to ensure that they comply with law and policy protecting USP privacy. TV's certification process evaluates system controls for maintaining compliance in a number of areas, including data tagging and data access.  |
| (U) NSA will conduct ongoing oversight activities and make any necessary reports, including those relating to incidents of non-compliance, to the NSA OIG and OGC, in accordance with the NSA charter.   | (U// <del>FOUO</del> ) SV and TV investigate incidents of non-compliance with FAA §702 targeting and minimization procedures. SV works with mission teams to document FAA §702 incidents. SV promptly reports potential incidents to OGC and ODOC and maintains a permanent record. When a potential incident involves a system, TV manages the incident investigation. |
|  | (U// <del>FOUO</del> ) The OIG receives notification of incident reports for all NSA authorities, including FAA §702. The OIG also receives Congressional notifications and notices filed with the FSSC of incidents of non-compliance with the FAA §702 targeting and minimization procedures.   |
|  | (U// <del>FOUO</del> ) OGC receives notifications of potential incidents of non-compliance for all NSA authorities. OGC compiles FAA §702 incidents daily (which it provides to DoJ NSD and ODNI), and assesses whether incidents represent possible non-compliance with the FAA §702 certifications and associated targeting and minimization procedures.              |

~~TOP SECRET//SI//NOFORN~~

|  |   |
|--|---|
| (U) NSA will ensure that necessary corrective actions are taken to address any identified deficiencies.  | (U//FOUO) SV and TV investigate all incidents of non-compliance with FAA §702 targeting and minimization procedures and monitor corrective actions.<br>(U) OIG performs audits and special studies of the FAA §702 program; tracks recommendations until completion.  |
| (U) NSA will conduct periodic spot checks of targeting decisions and intelligence disseminations to ensure compliance with established procedures, and conduct periodic spot checks of queries in data repositories. | (U//FOUO) SV performs oversight of targeting decisions, queries, and dissemination and provides documentation for review by DoJ NSD and ODNI to support their oversight of NSA's implementation of FAA §702. SV also conducts super audits of queries of raw SIGINT databases.<br>(U) OGC reviews all proposed disseminations of information constituting USPP attorney-client privileged communications before dissemination.    |
| (U//FOUO) NSA will report incidents of non-compliance with the targeting and minimization procedures within five business days of discovery to the DoJ NSD and ODNI OGC, and ODNI CLPO.                              | (U//FOUO) OGC notifies external overseers of incidents of possible non-compliance with the targeting procedures within five business days of discovery. OGC coordinates input by NSA organizations for Rule 13 notices prepared by DoJ NSD, in coordination with ODNI, for all violations of the FAA §702 targeting and minimization procedures.  |
| (U//FOUO) DoJ NSD and ODNI will oversee NSA's exercise of the FAA §702 authority, which will include bi-monthly reviews to evaluate the implementation of the procedures.  | (S//NF) DoJ NSD and ODNI perform bi-monthly reviews of NSA authorities under the [ ] FAA §702 certifications. DoJ NSD and ODNI review NSA's targeting decisions, including the source documentation supporting these determinations, to assess compliance with NSA targeting procedures and Attorney General's (AG) Acquisition Guidelines. NSD and ODNI also review queries, and disseminations of serialized reporting and EMT. |
| (U//FOUO) DoJ NSD and ODNI will oversee NSA's activities with respect to use of USP identifiers to query communications collected under FAA §702.  | (S//NF)   |

(S//NF)

(b)(1)  
 (b)(3) HPL 886386  
 (b)(3) 50 USC 3024(i)

### **(U) FAA §702 Incidents of Non-Compliance**

(U//FOUO) FISC Rules of Procedure require NSA to report to the FISC "corrections of material facts" and disclosures of non-compliance with FAA §702. In addition, NSA determines whether Congressional notifications are required.

### **(U) FISC Rules of Procedure**

(U//FOUO) The FISC Rules of Procedure govern FISC proceedings. Rule 13, *Correction of Misstatement or Omission; Disclosure of Non-compliance*, is the procedure NSA follows when notifying the Court through DoJ NSD of incidents of non-compliance with FAA §702.

**(U) Rule 13(a) Correction of Material Facts** If the government discovers that a submission to the Court contains a misstatement or omission of material fact, the

~~-TOP SECRET//SI//NOFORN~~

ST-14-0002

government must immediately, in writing, inform the Judge to whom the submission was made of:

- (1) (U) the misstatement or omission;
- (2) (U) necessary corrections;
- (3) (U) the facts and circumstances relevant to the misstatement or omission;
- (4) (U) modifications the government has made or proposes to make in how it will implement any authority or approval granted by the Court; and
- (5) (U) how the government proposes to dispose of or treat information obtained as a result of the misstatement or omission.

**(U) Rule 13(b) Disclosure of Non-compliance** If the government discovers that an authority or approval granted by the Court has been implemented in a manner that did not comply with the Court's authorization or approval or with applicable law, the government must immediately in writing, inform the Judge to whom the submission was made of:

- (1) (U) the non-compliance;
- (2) (U) the facts and circumstances relevant to the non-compliance;
- (3) (U) modifications the government has made or proposes to make in how it will implement any authority or approval granted by the Court; and
- (4) (U) how the government proposes to dispose of or treat information obtained as a result of the non-compliance.

#### **(U) Identifying and Reporting Incidents of Non-compliance**

##### **(U) Identifying incidents of non-compliance**

**(U//FOUO)** All potential incidents of non-compliance with FAAA §702 certifications and targeting and minimization procedures are reported to SV or TV upon discovery by analysts and others operating under the authority, as documented in the *FAA §702 Program Control Framework section -Incident Recognition and Reporting*. Training provides all personnel with awareness for personnel to identify potential violations. Incidents may also be discovered through oversight mechanisms addressed in the *FAA §702 Program Control Framework section Post-Targeting and Oversight*. Monitoring and oversight include manual and technical controls to detect abnormalities.

**(U//FOUO)** After review of the incident, SV or TV forwards documentation to OGC. If OGC believes a violation of the targeting and minimization procedures has or may have occurred, even if all the facts have not been gathered, preliminary notification is sent to DoJ NSD. OGC notifies DIRNSA of instances of non-compliance, as appropriate. Upon receiving initial notification from OGC, DoJ NSD drafts, in conjunction with ODNI, a notification to the Court, should one be required under the FISC Rules of Procedure.

~~-TOP SECRET//SI//NOFORN~~

(U//FOUO) Once the facts have been gathered and OGC has made an initial determination that a non-compliant FAA §702 event has occurred, OGC finalizes a notification of non-compliance and forwards it to DoJ NSD and ODNI, which make the final determination as to whether there has been an incident of non-compliance that must be reported to the FISC. If DoJ NSD and ODNI determine that an incident of non-compliance has occurred, DoJ drafts a notification, which is coordinated with the IC elements involved, finalizes it, and files the notice with the Court.

(U//FOUO) DoJ NSD often follows up on preliminary notifications with one or more additional notifications. In some cases, the preliminary notification of an incident serves as the final notice of that incident.<sup>99</sup>

(b)(3)-P.L. 86-366

(U//FOUO) In 20B, [ ] incidents of non-compliance (13(b)s) were filed with the FISC for material identified in that calendar year. None of these incidents involved inaccurate information in previously filed declarations to the Court, requiring that a Rule 13(a) notice of correction of material fact be filed.

#### (U) Congressional notifications

(U//FOUO) DIRNSA, as head of an IC element, has a statutory obligation to keep the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence fully and currently informed of all significant intelligence activities.<sup>100</sup> NSA resists doubts about notification in favor of notification. In addition to notifying Congress and the Director of National Intelligence, DIRNSA must notify the USD(I) and other USDoI staff, as directed by USD(I) guidance. For all FAA §702 incidents of non-compliance reported to Congress via the intelligence committees, NSA also provides discretionary notifications to the Senate and House Committees on the Judiciary.

(U//FOUO) NSA's LAO manages NSA's liaison with Congress and with the DNI, DoD, the IC, and the US Government departments and agencies regarding matters of concern to Congress. LAO is NSA's focal point for Congressional inquiries, correspondence, questions for record, and RRFs directed to NSA.

(U//FOUO) NSA/CSS Policy 1-33 provides guidelines for identifying matters that OGC and LAO must consider reporting to the Congressional intelligence committees under 50 U.S.C. §§3091 and 3092. The guidelines do not constitute a comprehensive list of what must be reported. Compliance incidents are assessed under a general guideline to consider reporting matters that the intelligence committees have

<sup>99</sup> (U//FOUO) DoJ NSD files the "Quarterly Report to the Foreign Intelligence Surveillance Court Concerning Compliance Matters Under Section 702 of the Foreign Intelligence Surveillance Act" which includes incidents DoJ NSD and ODNI determined to be violations of the targeting and minimization procedures (13(b)s) as well as all other incidents determined not to meet the reporting requirements of 13(b). This quarterly report to the FISC also provides supplemental information on previously reported compliance incidents.

<sup>100</sup> (U) 50 U.S.C. §3091, as implemented by Intelligence Community Directive 12, *Congressional Notification*, 16 November 2011, requires the head of each element of the IC to inform Congress on significant intelligence activities.

~~-TOP SECRET//SI//NOFORN~~

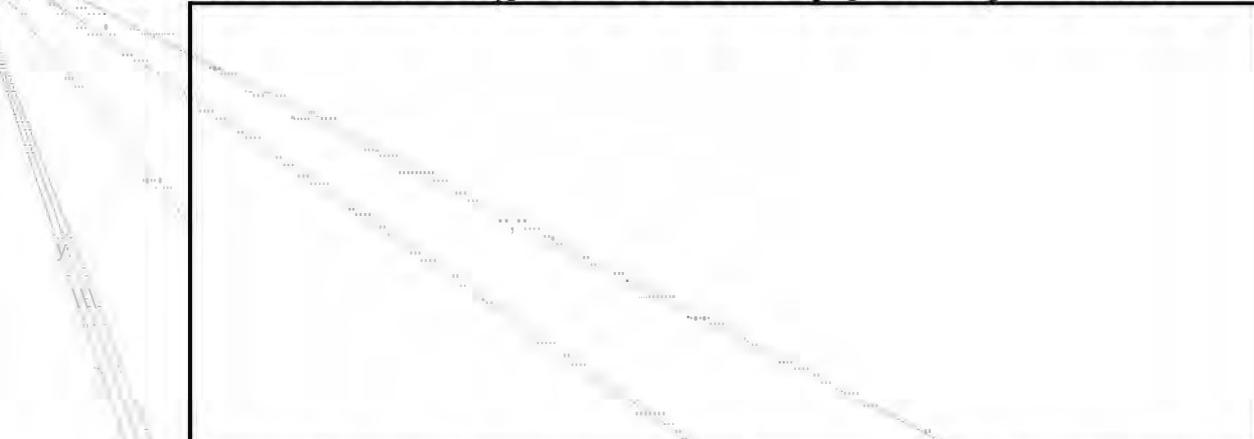
ST-114-00002

expressed accounting in interest in now which there is equally significant intelligence activities so failures.

(U//~~FOUO~~) NSA works to keep Congressional intelligence committees fully and currently informed about the Agency's activities even and above what is strictly required to be reported under the guidelines outlined in NSASSSS Policy 33. At a minimum, however, NSA must keep the Congressional intelligence committees timely informed of all major intelligence policies and activities and provide the information those Committees request.

(U//~~FOUO~~) Determining whether Congressional notification should be provided is a judgment based on the facts and circumstances and on the nature and extent of previous notifications to Congress on the same matter. Not every intelligence activity warrants Congressional notification. NSA's analysis of the FAA §702 incidents of non-compliance filed during 2013 resulted in two incidents reported in Congressional notifications; one related to a 2013 incident, and the other to an incident first reported in 2012.

(b)(1) ~~(TS//SI//NF)~~ Congressional Notification, [redacted] reported a retention and dissemination compliance incident involving NSA corporate database



~~(TS//SI//NF)~~ Congressional Notification, [redacted] provided resolution of a matter first reported to the Congressional intelligence committee on [redacted], [redacted]

[redacted] This update reported on the actions taken to resolve the matter, including correction of the affected system component(s) of affected transactions, verification that no disseminated report had been based upon overcollected data, and implementation of a post-acquisition review of this type of data to identify future overcollection.

<sup>101</sup> (U//~~FOUO~~) [redacted]

(b)(3)-P.L. 86-36 [redacted]

~~-TOP SECRET//SI//NOFORN~~

## (U) Incidents of Non-compliance in 2013 (b)(3)-P.L. 86-36

(U//FOUO) In 2013, DoJ reported to the Court [ ] incidents of non-compliance with FAA §702. The incidents and rates of occurrence are in Table 42.

**(U//FOUO) Table 42. FAA §702 Incidents of Non-Compliance Reported in 2013**

[TS//SI//NF]

| Incident Type                                  | Percentage |
|--|------------|
| Tasking Errors*                                | 12%        |
| Detasking Errors†                              | 19%        |
| Non-compliance with Notification Requirement‡  | 57%        |
| Non-compliance with Documentation Requirement§ | 5%         |
| Minimization Errors¶                           | 6%         |
| Other**  | 1%         |

\* (U) Tasking errors—foreignness support was insufficient to support tasking (e.g., foreignness was not reestablished following travel to the United States, foreign intelligence purpose explanation was insufficient, or a typographical error was made).

† (U) Detasking error examples include: (1) delayed detasking which occurs when NSA has a foreign intelligence target, reasonably believed to be outside the United States at the time of tasking and later learns that the target plans to travel to the United States, but does not detask the target's selectors before the target arrives in the United States; and (2) incomplete detasking of all tasked selectors when it is determined the target is no longer eligible for tasking.

‡ (U) Notification—NSA's targeting procedures require certain incidents to be reported to NSD and ODNI within five business days, even if these incidents do not involve non-compliance with the targeting procedures. Specifically, NSA is required to terminate acquisition and notify NSD and ODNI if "NSA concludes that a person is reasonably believed to be outside the United States and after targeting this person learns that the person is inside the United States, or if NSA concludes that a person who at the time of targeting was believed to be a non-United States person was in fact a United States person."

§ (U//FOUO) Documentation Errors—The targeting procedures require that NSA provide a citation to the source of information upon which the determination of the target's foreignness was made. These errors, in which the citations were not considered adequate to support the foreignness of the user of the selector tasked, were identified through DoJ and ODNI review of NSA tasking.

¶ (U) Minimization errors may include errors in querying, reporting, and retention.

\*\* (U) The "other" incident type often pertains to instances in which systems that support compliance are not operating as intended.

[TS//SI//NF]

(U//FOUO) Examples of incidents, including actions NSA took to mitigate recurrence, follow. This information is taken from the 13(b) notices DoJ NSD filed with the FISC.

**(U//FOUO) Example 1: Incident as a result of delayed detasking**

**[REDACTED] Non-Compliance Incident Regarding Section 702-Tasked [REDACTED]**

(S//SI//NF) [REDACTED] NSA reported to the National Security Division (NSD) and the Office of the Director of National Intelligence (ODNI) a delay in the detasking of

~~TOP SECRET//SI//NOFORN~~

ST-14-0002

(b)(1)

(b)(3)-P.L. 86-36

(b)(3)-50 USC 3024(i)



(b)(1) (S//SI//NF) [REDACTED] NSA determined [REDACTED] that the (b)(3)-P.L. 86-36 targeted user of [one of the selectors] had traveled to the U.S. [REDACTED] [REDACTED] an NSIA analyst detasked [the selector associated with the U.S. travel]. The analyst, however, inadvertently did not detask the other [REDACTED] [REDACTED] selector used by the target. NSA discovered this effort [REDACTED] and de tasked [REDACTED] the same day. The continued tasking of the [remaining selector] was not discovered until [REDACTED] when [the selector] was immediately de tasked.

(U//FOUO) Action taken to mitigate recurrence The target office [was] reminded of the need to identify and immediately de task all facilities used by a target when the target is found to be in the United States.

(U//FOUO) NSA did not issue a Congressional notification about this incident. The incident was included in the *Semiannual Report of the Attorney General Concerning Acquisitions under Section 702 of the Foreign Intelligence Surveillance Act*, dated March 2014.

(U//FOUO) Example 22: Other incident (technical error)

(b)(1)  
(b)(3)-P.L. 86-36

(b)(1)  
(b)(3)-P.L. 86-36

(S//NF) Preliminary [REDACTED] NSA orally notified the NSD of an incident regarding the [REDACTED] post-tasking checks NSA conducts to help ensure that [REDACTED] accounts tasked for collection pursuant to Section 702 are not being used from inside the U.S. NSA provided written notice of this incident to NSD and the ODNI [REDACTED]

(S//NF) NSA identified the following compliance incident as a result of its ongoing [REDACTED]

(S//NF) NSA's post tasking [REDACTED] checks are intended to identify indications that users of Section 702-tasked [selectors] may be inside the U.S. [REDACTED]

(b)(1)  
(b)(3)-P.L. 86-36

~~TOP SECRET//SI//NOFORN~~

(b)(1)

(b)(3)-P.L. 86-36

(b)(3)-50 USC 3024(i)

(b)(1)  
(b)(3)-P.L. 86-36  
(b)(3)-50 USC 3024(i)  
(b)(3)~ ~ SO ~

[redacted]  
and confirmed that there is no [redacted]

[redacted] NSA, NSD, and ODNI [at the time] continue[d] to investigate this incident. The Department of Justice [committed] to continue to inform the Court of additional information regarding this incident as it became available.

**(S//NF) Supplement/Final** As detailed in the preliminary notice... NSA determined that certain Section 702 [selectors] were not being sent from NSA's [redacted]

[redacted] to NSA's [redacted]

[redacted] thereby preventing [redacted] post-tasking  
[redacted] from being conducted regarding these [selectors]. [redacted]

(b)(1)  
(b)(3)-P.L. 86-36  
(b)(3)-50 USC 3024(i)

(b)(1)~ ~ ~ ~ ~  
(b)(3)-P.L. 86-36

(S//NF) NSA made a modification to ensure that [redacted]

SA

[redacted] NSA [at that time] continued to investigate the alert [redacted]

[redacted] potential for a future compliance incident. NSA has corrected the error that prevented [redacted]

TOP SECRET//SI//NOFORN

~~-TOP SECRET//SI//NOFORN~~

ST-14-0002

(b)(1)  
(b)(3)-P.L. 86-36

[redacted] while those facilities were tasked for Section 702 acquisition. With respect to the remaining [redacted] (selectors), NSA has identified one confirmed period of roaming in the United States by the intended target, which lasted [redacted] days.

[redacted] accounts have been de-tasked.

(b)(1)  
(b)(3)-P.L. 86-36  
(b)(3)-50 USC 3024(i)

(S//SI//NF) Summary of action taken to mitigate recurrence. With respect to [redacted] (S//SI//NF) [redacted] (selectors) discussed above, NSA advised that the unique identifiers associated with communications acquired while users were overseas may have been in the U.S. were added to NSA's Master Purge List (MPL) in discover status.<sup>107</sup> [redacted]

(S//NF) The notice also stated that DOJ would include this issue in its quarterly report to the Court regarding Section 702 compliance occurrences and that the report would confirm that NSA had added the communications to the MPL in purge state.

(U//FOUO) NSA did not issue a Congressional notification about this incident. The preliminary incident of non-compliance was included in the *Semiannual Report of the Attorney General Concerning Acquisitions under Section 702 of the Foreign Intelligence Surveillance Act*, dated March 2014.

#### **(U) NSA Use of the FAA §702 Authority**

(b)(1)  
(b)(3)-P.L. 86-36

(S//NF) NSA asserts that the FAA's §702 authority provides significant foreign intelligence information related to the foreign intelligence categories specified in the [redacted] FAA §702 certifications. The [redacted] certifications cover [redacted]

(b)(1)  
(b)(3)-P.L. 86-36  
(b)(3)-50 USC 3024(i)

#### **(U) Methods Used to Assess Effectiveness**

(U//FOUO) NSA maintains a variety of statistics related to the FAA §702 authority that show the overall contributions to NSA SIGINT reporting, how customers value and use reports, and the unique access to foreign intelligence information FAA §702 provides. Data presented in this report is for calendar year 2013, unless otherwise noted, and statistics are limited to NSA reporting.

#### **(U) FAA §702 contributions to SIGINT reporting**

(b)(1)  
(b)(3)-P.L. 86-36

(TS//SI//REL TO USA, FVEY) As Figures 9 and 10 show, information obtained under FAA §702 is a key and growing source of reportable foreign intelligence to U.S. government consumers and allied foreign governments. Of the more than [redacted] SIGINT reports issued in calendar year 2013, [redacted] percent were based in whole or in part on FAA §702 information.

<sup>107</sup> (S//NF)

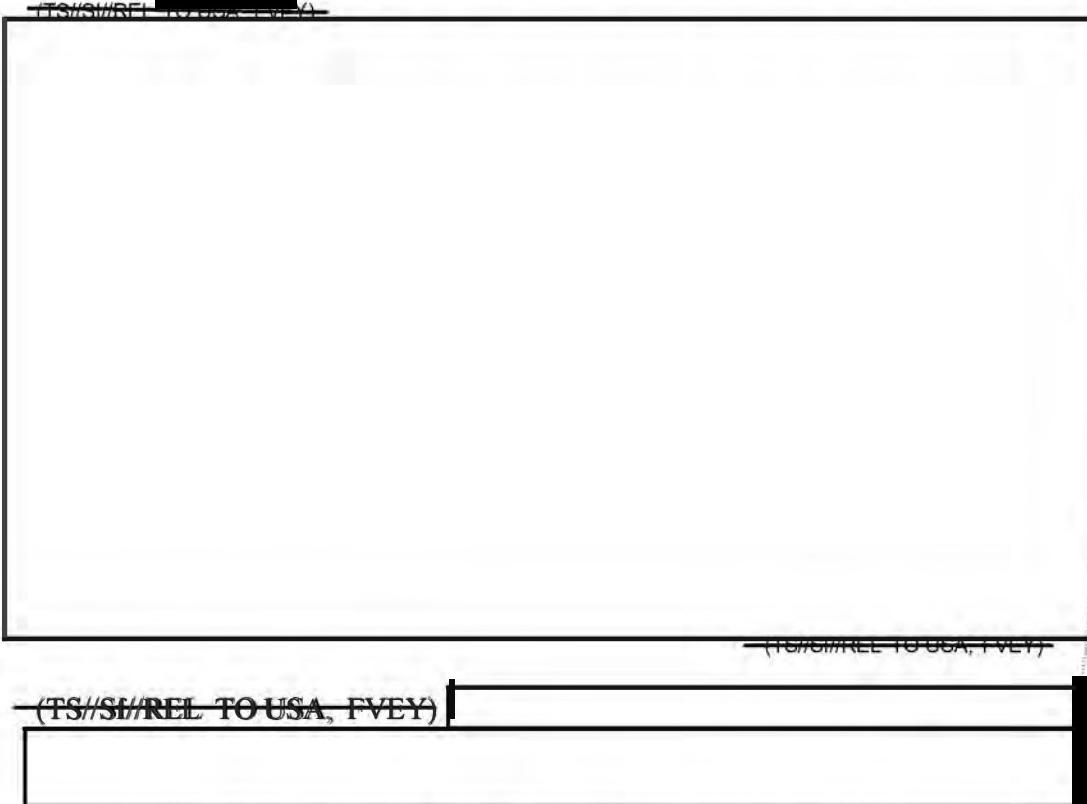
(b)(1)

(b)(3)-P.L. 86-36

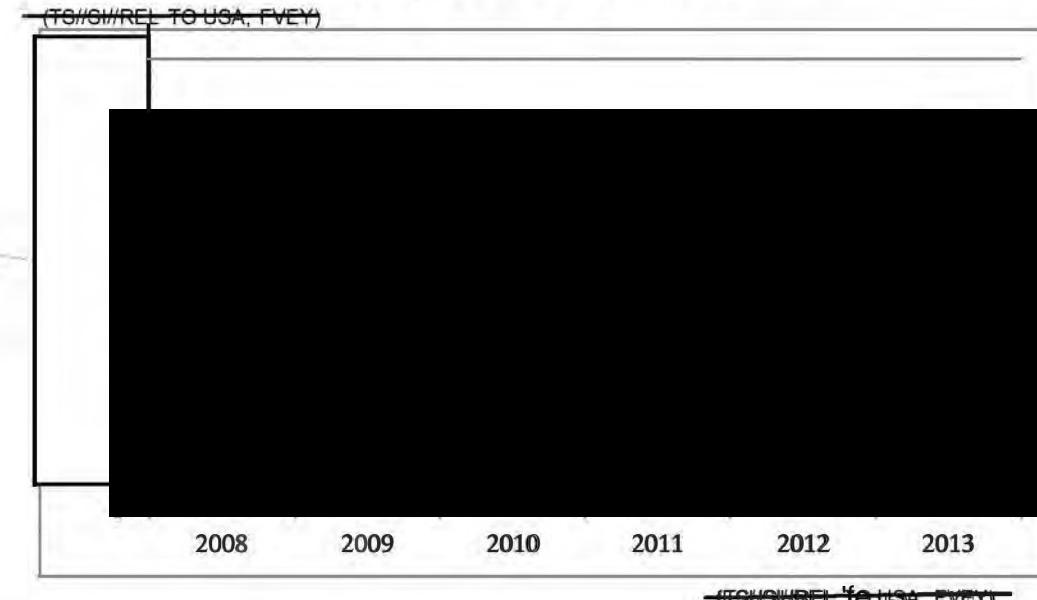
~~-TOP SECRET//SI//NOFORN~~

~~TOP SECRET//SI//NOFORN~~

ST-14-0002

(U) Figure 9. Total SIGINT Reports Issued<sup>108</sup> by Year

(U) Figure 10. SIGINT Reports Based in Whole or in Part on FAA SS7022 or PAA Collection



<sup>108</sup> (C//REL TO USA, FVEY) When a report is solely sourced to an authority, it indicates that a particular source was used by the analyst but does not mean that the collection was only available from that one source of collection.

~~TOP SECRET//SI//NOFORN~~

~~TOP SECRET//SI//NOFORN~~

ST-14-0002

(TS//SI//REL TO USA, FVEY) During 2013, NSA disseminated an average of over [redacted] serialized SIGINT reports a month that included information collected under the FAA §702 certifications.<sup>109</sup> [redacted]

(b)(1)

(b)(3)-P.L. 86-36 (S//SI//REL TO USA, FVEY) NSA management believes that disseminated reports based on FAA §702 collection further the U.S. government's understanding of high priority international terrorism targets. Beyond disseminated reports, collection obtained under FAA §702 contributes to [redacted] and helps intelligence analysts [redacted]. J [redacted]

(TS//SI//REL TO USA, FVEY) On average, during 2013 NSA disseminated [redacted] D SIGINT reports per month concerning international terrorism that include information derived from FAA §702 collection.

**(U) Figure 11. Terrorism-Specific SIGINT Reports Collected with FAA §702 Information CY2013**

(TS//SI//REL TO USA, FVEY)

(b)(1)

(b)(3)-P.L. 86-36

(TS//SI//REL TO USA, FVEY)

<sup>109</sup> (U//FOUO) The number of issued reports was obtained in November 2014 from NSA's management information system for SIGINT production. The number of reports for any period is net of any reports recalled after they were issued.

~~TOP SECRET//SI//NOFORN~~

TOP SECRET//SI//NOFORN

ST-14-0002

(TS//SI//NF) On average, more than [redacted] selectors were tasked for acquisition under FAA §702 during 2013. [redacted]

(b)(1)  
(b)(3)-P.L. 86-36

#### (U) Analyst Use of the Authority

(S//NF) The FAA §702 authority is utilized broadly to support NSA missions. Its usefulness is confirmed by the above statistics, as well as the fact that the number of selectors tasked to the authority has increased [redacted] since 2010. Similarly, the increase in the number of reports sourced by FAA §702 communications has increased [redacted] in the same period.

#### (U) FAA §702 Contributions to the Intelligence Mission

(U) In 2013, NSA reported to the Senate Committee on Intelligence that "information gathered from Section 702 of the FISA Amendments Act and Section 215 of the Patriot Act, in complement with NSA's other authorities, has contributed to the United States government's understanding of terrorist tactics and, in many cases, has enabled the disruption of potential terrorist events at home and abroad."

(U) On 21 June 2013, NSA provided to several Congressional committees testimony concerning 54 cases in which these programs contributed to the U.S. government's understanding and, in many cases, disruption of terrorist plots in the United States and more than 20 countries.

(U) The SIGINT Directorate provided to the OIG additional examples of the value of FAA §702 collection to NSA missions.

(b)(1)-P.L. 86-36  
" " -P.L. 86-36

(TS//SI//NF) 1

(b)(1)  
(b)(3)-P.L. 86-36  
(b)(3)-18 USC 798  
(b)(3)-50 USC 3024(i)

(b)(4)  
(b)(3)-P.L. 86-36

(b)(1)  
(b)(3)-P.L. 86-36  
(b)(3)-18 USC 798  
(b)(3)-50 USC 3024(i)

TOP SECRET//SI//NOFORN

~~-TOP SECRET//SI//NOFORN~~

ST-14-0002

1

(TS//SI//NF)

(b)(1)  
(b)(3)-P.L. 86-36  
(b)(3)-18 USC 798  
(b)(3)-50 USC 3024(i)

(TS//SI//NP) Section 702

(TS//SI//NF) Section 702.1-

(TS//SI//NF) Based on Section 702 collection [redacted] disrupted the potential attack

(SFS#SI//NF)

(b)(1)  
(b)(3)-P.L. 86-36  
(b)(3)-18 USC 798  
(b)(3)-50 USC 3024(i).

(TS//SI//NF)

~~-TOP SECRET//SI//NOFORN~~

~~-TOP SECRET//SI//NOFORN~~

ST-14-0002

(TS//SI//REL TO USA, p) EJC [REDACTED] based upon information obtained  
[REDACTED] pursuant to Executive Order 12333 and Section 702, NSA [REDACTED]

(TS//SI//REL TO USA, FVEY) Section 702 [REDACTED]

(TS//SI//NF) [REDACTED]

(TS//SI//NF) [REDACTED]

{b} (f)

(b)(1)

(b)(3)-P.L. 866366

[REDACTED] had been arrested [REDACTED]

~~-TOP SECRET//SI//NOFORN~~

~~TOP SECRET//SI//NOFORN~~

ST-14-0002

(S//REL TO US//AIL-r=====')....

(S//SI//REL TO USA

(b)(1) (b)(3)-P.L. 86-36



[Redacted]

(b)(1)

(b)(3)-P.L. 86-36

(b)(3)-18 USC 798

(b)(3)-50 USC 3024(i)

~~TOP SECRET//SI//NOFORN~~

**IV. (U) ABBREVIATIONS AND ORGANIZATIONS**

|                    |   |
|--------------------|---|
| (U) ADET           | Associate Directorate for Education and Training  |
| (U) AIG            | Authorities Integration Group                     |
| (U) L-1            | L   |
| (U) ATSD(10)       | Assistant to the Secretary                        |
| (U) [redacted]     | [redacted]  |
| (U) BMD            | Bulk metadata                                     |
| (U) BR             | Business Records                                  |
| (U) [redacted]     | [redacted]  |
| (U) CDR            | Call Detail Record                                |
| (U) CIA            | Central Intelligence Agency                       |
| (U) CMCP           | Comprehensive Mission Compliance Program          |
| (U) CSLI           | Cell site location information                    |
| (U) CSP            | Communication Service Provider                    |
| (U) CT             | Counterterrorism                                  |
| (U) DIA            | Data Integrity Analyst                            |
| (U) DIRNSA         | Director, NSA                                     |
| (U) DMR            | Dataflow Management Request                       |
| (U) DNI            | Director of National Intelligence                 |
| (U) DoD            | Department of Defense                             |
| (U) DoJ NSD        | Department of Justice, National Security Division |
| (U) DTM            | Directive Type Memorandum                         |
| (U) DTOI           | Date and Time of Intercept                        |
| (U) EAR            | Emphatic Access Resolution                        |
| (U) EDH            | Enterprise data header                            |
| (U) [redacted], 1. | [redacted] 1.                                     |
| (U) E.O.           | Executive Order                                   |
| (U) FAA            | FISA Amendments Act                               |
| (U) FBI            | Federal Bureau of Investigation                   |
| (U) FISA           | Foreign Intelligence Surveillance Act             |
| (U) FISC           | Foreign Intelligence Surveillance Court           |
| (U) FTP            | File Transfer Protocol                            |
| (U) [redacted]     | [redacted]  |
| (U) [redacted]     | [redacted]  |
| (U) HMC            | Homeland Mission Coordinator                      |
| (U) IC             | Intelligence Community                            |
| (U) IMEI           | International Mobile Station Equipment Identity   |
| (U) IMSI           | International Mobile Subscriber Identity          |
| (U) IO             | Intelligence Oversight                            |
| (U) LAO            | Legislative Affairs Office                        |
| (U) MCT            | Multiple Communication Transaction                |

(b)(1)  
(b)(3)-P.L. 866366

TOP SECRET//SI//NOFORN

ST-14-0002

|                |  |
|----------------|--|
| (U) MIPL       | Master Purge List  |
| (U) MIRG       | Math Research Group  |
| (U) [REDACTED] | [REDACTED]   |
| (U) NCCTC      | National Counterterrorism Center                           |
| (U) NSA        | National Security Agency/Central Security Service          |
| (U) NSAW       | NSA Washington   |
| (U) NSD        | National Security Division                                 |
| (U) NSOC       | National Security Operations Center                        |
| (U) ODNI       | Office of the Director of National Intelligence            |
| (U) ODOC       | Office of the Director of Compliance                       |
| (U) OGC        | Office of General Counsel                                  |
| (U) OIG        | Office of the Inspector General                            |
| (U) OTR        | Obligation to Review                                       |
| (U) PKI        | Public key infrastructure                                  |
| (U) Q          | Associate Directorate for Security and Counterintelligence |
| (U) RAS        | Reasonable Articulable Suspicion                           |
| (U) RFI        | Request for information                                    |
| (U) [REDACTED] | [REDACTED]   |
| (U) S1S        | Information Sharing Services Group                         |
| (U) S2         | Information Sharing Services Group                         |
| (U) S2I        | Analysis and Production                                    |
| (U) S2I4       | Counterterrorism Production Center                         |
| (U) S3         | Homeland Security Analysis Center                          |
| (U) S31324     | Data Acquisition   |
| (U) S31324     | [REDACTED]   |
| (U) S354       | [REDACTED]   |
| (U) SCA        | Special compliance activity                                |
| (U) SCIF       | Sensitive Compartmented Information Facility               |
| (U) [REDACTED] | [REDACTED]   |
| (U) SID        | Signals Intelligence Directorate                           |
| (U) SIGINT     | Signals Intelligence                                       |
| (U) [REDACTED] | [REDACTED]   |
| (U) SOO        | Senior Operations Officer                                  |
| (U) [REDACTED] | [REDACTED]   |
| (U) HO         | [REDACTED]   |
| (U) SV         | [REDACTED]   |
| (U) T12        | [REDACTED]   |
| (U) T12222     | [REDACTED]   |
| (U) T1311      | [REDACTED]   |
| (U) T1B323     | [REDACTED]   |
| (U) T16        | [REDACTED]   |
| (U) TD         | Technology Directorate                                     |
| (U) TR         | Targeting request  |
| (U) TS         | [REDACTED]   |

(b)(1)  
(b)(3)-P.L. 86-36

TOP SECRET//SI//NOFORN

TOP SECRET//SI//NOFORN

ST-14-0002

(U) [ ]

(U) TV

(U) TV4

(U) USD(I)

(U) USP

(U) USSID

(U) USSS

(U) [ ]

(U) VOA

[ ]

DO Office of Compliance

Compliance and Verification

Undersecretary of Defense for Intelligence

U.S. person

U.S. Signals Intelligence Directive

U.S. SIGINT System

[ ]

Verification of accuracy

(b)(3):PL: 86-36

TOP SECRET//SI//NOFORN

**(U) APPENDIX A: ABOUT THE §215 AND FAA §702 REVIEW****(U) Reason for Review**

**(U//FOUO)** In September 2013, members of the Senate Committee on the Judiciary requested a comprehensive, independent review of the implementation of §215 of the USA PATRIOT Act and §702 of the Foreign Intelligence Surveillance Act (FISA) Amendments Act (FAA) of 2008 for calendar years 2000 through 2013.

**(U) Objectives**

**(U//FOUO)** In January 2014, the National Security Agency/Central Security Service's (NSA) Office of the Inspector General (OIG) and Committee staff agreed that the NSA OIG would review NSA's implementation of both authorities for calendar year 2013. The study has three objectives:

**(U) Objective I**

- (U) Describe how data was collected, stored, analyzed, disseminated and retained under the procedures for §215 and FAA §702 authorities in effect in 2013 and the steps taken to protect US Person information.
- (U) Describe the restrictions on using the data and how those restrictions have been implemented including a description of the data repositories and the controls for accessing data.
- (U) Describe oversight and compliance activities performed by internal and external organizations in support of §215 Foreign Intelligence Surveillance Court (FISC) Orders and FAA §702 minimization procedures.

**(U) Objective III**

- (U) Describe incidents of non-compliance with §215 FISC Orders and FAA §702 Certifications and what NSA has done to minimize recurrence.

**(U) Objective IIII**

- (U) Describe how analysts used the data to support their intelligence missions.

**(U//FOUO)** The report also provides a summary of the changes made in the implementation of both authorities for calendar years 2000 through 2012 and for §215, a list of incidents of non-compliance for calendar years 2010 through 2012.

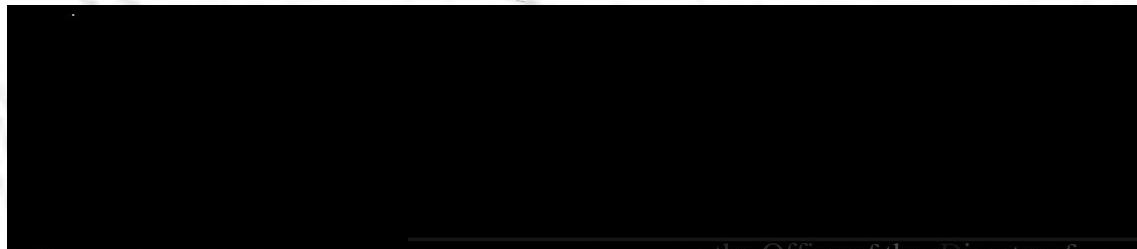
**(U) Scope and Methodology**

(U//~~FOUO~~) Our study of NSA's implementation of the §215 and FAA §702 authorities was based largely on program stakeholder interviews and reviews of policies and procedures and other program documentation. For this review, the NSA OIG documented the controls implemented that address the requirements of each authority. However, we did not verify through testing whether the controls were operating as described by program stakeholders.

**(U) Section 215**

(U//~~FOUO~~) Our §215 review focused on the BR FISA program control framework, incidents of non-compliance, and NSA's use of the authority to support its counterterrorism (CT) mission in 2013. To document the BR FISA control framework, we used BR Order 13-158, approved by the HISC on 11 October 2013 and effective through 30 January 2014, and compared the requirements listed in that Order with the processes and controls NSA used to maintain compliance with that Order. In addition, we documented the changes implemented in the BR FISA program following the President's directives in 2014.

(b)(3)-P.L. 86-36



the Office of the Director of Compliance (ODOC), the Authorities Integration Group (AIG); the Legislative Affairs Office (LAO); and the Office of General Counsel (OGC).

**(U) FAA §702**

(TS//~~SWIP~~) In addition to FAA §702 stakeholder interviews and reviews of policies and procedures and other program documentation, information obtained in the OIG's *Assessment of Management Controls Over FAA §702*, revised and reissued 29 March 2013, was also used as a resource. That review examined the controls that NSA used to maintain compliance with FAA §702 and the targeting and minimization procedures associated with the 2011 certifications.

(TS//~~SIMINT~~) Our FAA §702 review focused on the processes and controls in place in 2013. Two primary documents filed annually with each FAA §702 certification comprise NSA's procedures for complying with the FISAA and the FISA Act of 2008:

- (U//~~FOUO~~) *The Procedures Used by the National Security Agency for Targeting Non-United States Persons Reasonably Believed to be Located Outside the United States to Acquire Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended (FAA §702 Targeting Procedures)*, and

ST-14-0002

- (U//~~FOUO~~) The *Minimization Procedures Used by the National Security Agency in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended* (the FAA §702 Minimization Procedures).

(U//~~FOUO~~) For calendar year 2013, the period under review, different versions of these documents were in effect because of changes made with the annual certification renewal and special amendments.

- (U//~~FOUO~~) FAA §702 Targeting Procedures
  - (U//~~FOUO~~) Procedures approved with the 2012 renewal of the authority, effective 24 September 2012
  - (U//~~FOUO~~) These procedures were not changed for the 2013 certification renewal and remained effective 10 September 2013 through 9 September 2014.
- (U//~~FOUO~~) FAA §702 Minimization Procedures
  - (S//~~NF~~) Procedures approved for the 2012 certification renewal, approved by the FISC 24 August 2012, were effective 24 September 2012 through 23 September 2013.

(b)(1)  
(b)(3)-P.L.866386

(U//~~FOUO~~) We also examined implementing procedures and controls for the Attorney General's targeting guidelines.

(U//~~FOUO~~) We interviewed personnel in SID Policy and Corporate Issues Staff (S02), SW Analysis and Production (S02 Staff and Product Lines, Data Acquisition (S3)).

[redacted]  
[redacted]

[redacted]  
[redacted] and Mission Capabilities (T-1), QDOC, the LAO, and OGC.

#### **(U) Prior Coverage**

(b)(3)-P.L.866386

(U//~~FOUO~~) Since 24 May 2006, the date the original BR Order was signed, the NSA OIG has completed five BR FISA program reviews. Table A-1 summarizes the reviews the NSA OIG has performed on the BR FISA program.

TOP SECRET//SI//NOFORN

ST-14-0002

## (U) Table A-1. NSA OIG Reviews of the BRFISA Program

(S//SI//NF)

| Date Issued | OIG Review   | Scope of the Review   |
|-------------|--|---|
| 09/05/06    | Assessment of Management Controls for Implementing the FISC Order: Telephony BR (ST-06-0018) | Reviewed collection, processing, analysis, dissemination, and oversight controls.   |
| 05/12/10    | NSA Controls for FISC BR Orders (ST-10-0004)   | Reviewed querying and dissemination controls; summarized pilot test results for the period from January through March 2010.     |
| 05/25/11    | Audit of NSA Controls to Comply with the FISC Order Regarding BBR (ST-10-0004L)*             | Reviewed querying and dissemination controls; summarized the monthly test results for 2010.                                     |
| 10/20/11    | Audit of NSA Controls to Comply with the FISC Order Regarding BBR Retention (ST-11-0011)     | Verified age-off of BR FISA metadata in 2011 to maintain compliance with the 60 month retention requirement of the BR Order.    |
| 08/01/12    | NSA Controls to Comply with the FISC Order Regarding BR Collection (ST-12-0003)              | Reviewed collection and sampling controls for ensuring that NSA receives only the BR FISA metadata authorized by the BBR Order. |

\* This report summarizes monthly test results of the BBR querying and dissemination controls during 2010.

(T//SI//NF)

(U//FOUO) Since the Agency obtained FAA §702 authority in January 2008, the NSA OIG has completed annual reviews of five reports containing references to USP identities and targets later determined to be located in the United States, as required by the statute. Table A-2 summarizes the two reviews the NSA OIG has completed of the FAA §702 program.

## (U) Table A-2. NSA OIG Reviews of the FAA §702 Program

(S//SI//F)

| Date Issued | OIG Review   | Scope of the Review   |
|-------------|--|---|
| 3/29/13     | (U) Assessment of Management Controls Over FAA §702 (ST-11-0009) | (U//FOUO) Reviewed management controls for maintaining compliance with the targeting and minimization procedures. |
|             | (S//NF)  | (S//NF)   |

(S//SI//F)

(b)(1)

(b)(3)-P.L.866386

TOP SECRET//SI//NOFORN

ST-14-0002

**(U) APPENDIX B: BR FISA PROGRAM CHANGES  
2010-2012**

**(U) 2010**

- (U//FOUO) On 25 June 2010, [REDACTED] NSA's RAS selection term management system. [REDACTED]
- (U//FOUO) [REDACTED] the Order requirement restricting the number of analysts allowed to access BR metadata was lifted.
- (U//FOUO) [REDACTED] the Order requirement for weekly reports of BR-related disseminations was changed to monthly.

(b)(3)-P.L. 86-36

**(U) 2011**

- (U//FOUO) [REDACTED] primary repository for detailed telephony transaction records.. [REDACTED]

**(U) 2012**

- (U//FOUO) [REDACTED] the Order requirement for NSA to review a sample of records obtained was changed to a review of NSA's monitoring and assessment to ensure that only approved metadata is being acquired.
- (U//FOUO) [REDACTED] NSA notified the Court [REDACTED].  
[REDACTED]
- (U//FOUO) [REDACTED] NSA notified the Court [REDACTED].  
[REDACTED]
- (U//FOUO) [REDACTED] the Court authorized NSA to implement an automated querying process.<sup>110</sup>

<sup>110</sup> (U//FOUO) NSA is no longer authorized to use the automated query process since it withdrew its request to do so in the renewal applications and declarations that support the BR Orders approved by the FISC (beginning with BR Order 14-67, dated 28 March 2014).

~~-TOP SECRET//SI//NOFORN-~~

ST-14-0002

- (U//~~FOUO~~) On 29 November 2012, the Order requirement to track and report the number of instances, since the preceding report, in which NSA has shared, in any form, results from queries of the BR metadata, in any form, with anyone outside NSA was changed to apply to only sharing of query results that contain U.S. person information.

~~-TOP SECRET//SI//NOFORN-~~

~~-TOP SECRET//SI//NOFORN-~~

ST-14-0002

**(U) APPENDIX C: BR FISA PROGRAM INCIDENTS OF  
NON-COMPLIANCE 2010 THROUGH 2012****(U) Table C-1. BR FISA Incidents 2010 through 2012**

| Congressional<br>Notification | Description |
|-------------------------------|-------------|
|                               |             |

\* (U//FOUO) On 1 November 2010, Rule 10(b) and 10(c) notices were replaced by Rule 13(a) and 13(b) notices respectively.

† (U//FOUO) Final Rule 10(c) notice [REDACTED]

‡ (U//FOUO) Supplemental Rule 13(b) notice [REDACTED]

§ (U//FOUO) Final Rule 13(a) and 13(b) notice [REDACTED]

(b)(3)-P.L. 86-36

~~(TOP SECRET//NF)~~~~-TOP SECRET//SI//NOFORN-~~

(U) APPENDIX D: FAA §702 PROGRAM CHANGES

## **(U) Minimization Procedures**

(U) 2011

- (U//~~FOUO~~) Language on upstream data added to Minimization Procedures.
  - (U//~~FOUO~~) The retention period for Upstream Data is reduced to two years
  - (U//~~FOUO~~) Clarified that the five-year retention period for unevaluated data began to run from the date of expiration of the certification under which the data was collected. Prior versions did not specify when the five-year period began.
  - (U//~~FOUO~~) Permitted agencies using USPP identifiers to identify and select communications. Requires preapproval before any queries are made. Specifically excludes querying upstream data.
  - (U//~~FOUO~~) Adds requirement to segregate Internet transaction that cannot be reasonably identified as containing single discrete communications.

(U) 2012

- (U//~~FOUO~~) Limited access to metadata from Internet transactions to data acquired on or after October 31, 2011.
  - (U//~~FOUO~~) Adds specific requirements for DIRNSA determination that a domestic communication can be retained. This includes a requirement that DIRNSA first determine that the sender or recipient of the domestic communication was properly targeted under FAA §702.

{"6"}(1T)

(b)(3)-P.L. 86-36

~~• ("S) iEE ifOUA~~

(U) 2013

- (U) An amendment to the Minimization procedure was made in late 2013. A section was added precluding NSA from using information acquired pursuant to FAA §702 unless NSA determines, based on the totality of the circumstances, that the target is reasonably believed to be outside the United States at the time the information was acquired.

(b) (i-1)

(b)(3)-PL 86-36

(b)(3)-50 USC 3024(i))

~~(S/REL TO US AIR~~

(b)(1)  
(b)(3)-P.L.866366

~~TOP SECRET//SI//NOFORN~~

ST-14-0002

**(U) Other Changes****(U) 2012**

- ffs/fSi/F?W) Congress notified by NSA

//

(b)(1)  
(b)(3)-P.L.866366

(b)(1)  
(b)(3)-P.L.866366  
(b)(3)-50 USC 3024(i)

~~TOP SECRET//SI//NOFORN~~